APPENDIX E

This appendix shows some of the past COMSEC posters which have been produced by past COMSECers. The order of the posters is chonologic.

WAR DEPARTMENT
OFFICE OF THE CHIEF SIGNAL OFFICER
WASHINGTON

Y O U A R E

GIVING AID TO THE ENEMY

IF YOU DO THIS:

"ON SEPTEMBER 19, 1914, AN INTERCEPTED RUSSIAN WIRELESS MESSAGE WAS DECIPHERED BY THE AUSTRIAN INTELLIGENCE SERVICE FOR THE FIRST TIME. FROM THIS TIME UNTIL THE END OF THE WAR (FOR RUSSIA), MESSAGES SENT IN CIPHER BY THE RUSSIAN RADIO STATIONS IN THE FIELD WERE REGULARLY INTERCEPTED AND SUCCESSFULLY DECIPHERED BY THE EXPERTS OF THE AUSTRIAN INTELLIGENCE SERVICE. THE CONTENTS OF THESE MESSAGES WERE KNOWN TO THE AUSTRIAN AND GERMAN HIGH COMMANDS WITHIN A FEW HOURS AFTER TRANSMISSION." -- (GEN. MAX RONGE, FROM HIS "KRIEG UND INDUSTRIE SPIONAGE").

B E C A U S E

WHENEVER THE RUSSIANS CHANGED FROM ONE SYSTEM TO A NEW ONE (OR EVEN FROM ONE KEY TO ANOTHER), THEY INVARIABLY CRYPTOGRAPHED IDENTICAL PLAIN-TEXT MESSAGES IN BOTH SYSTEMS (OR IN BOTH KEYS). THIS IS NOT MERELY FOOLISH, --

I T ' S S U I C I D E

MORAL: NEVER CRYPTOGRAPH A MESSAGE IN A SYSTEM OR KEY OTHER THAN THAT IN WHICH IT HAS BEEN PREVIOUSLY TRANSMITTED.

DISSEMINATION OF THIS INFORMATION TO ALL PERSONNEL OF YOUR COMMAND IS DESIRED.

SSBR OCSIGO 10-22-42

OFFICE OF THE CHIEF SIGNAL OFFICER
WASHINGTON

FALSE ADDITION

1 MESSAGE + 2 SYSTEMS = 1 MESS

HOW IT HAPPENS

"ON MARCH 11, 1918, THE GERMANS BEGAN THE GENERAL USE OF A NEW CODE OF WHICH THE ALLIES HAD NO KNOWLEDGE... IT WAS REGARDED AS A FORERUNNER OF THE LONG-EXPECTED GERMAN OFFENSIVE. ON MARCH 13, WE RECEIVED A COPY OF A MESSAGE IN THE NEW CODE. THE ANSWER WAS IN AN OLD CODE WHICH WE COULD READ. IT WAS A REQUEST THAT THE FIRST MESSAGE BE REPEATED IN THE OLD CODE AS THE NEW CODE BOOKS HAD NOT BEEN RECEIVED. A FEW MINUTES LATER A MESSAGE FROM THE FIRST STATION IN THE OLD AND KNOWN CODE WAS RECEIVED. IT WAS COMPARED WITH THE FIRST MESSAGE AND FOUND TO CORRESPOND IN EVERY PARTICULAR. THIS NOT ONLY GAVE THE MEANING OF EVERY CODE GROUP IN THE FIRST MESSAGE, BUT INDICATED THE SYSTEM USED." ("MILITARY INTELLIGENCE IN THE A.E.F.," BY MAJOR GENERAL D. E. NOLAN, U. S. A.

WHY IT HAPPENS

WHEN THE GERMANS CHANGED FROM ONE SYSTEM TO ANOTHER (OR EVEN FROM ONE KEY TO ANOTHER), THEY CRYPTOGRAPHED IDENTICAL PLAIN-TEXT MESSAGES IN BOTH SYSTEMS (OR IN BOTH KEYS), AND THUS COMPROMISED BOTH SYSTEMS.

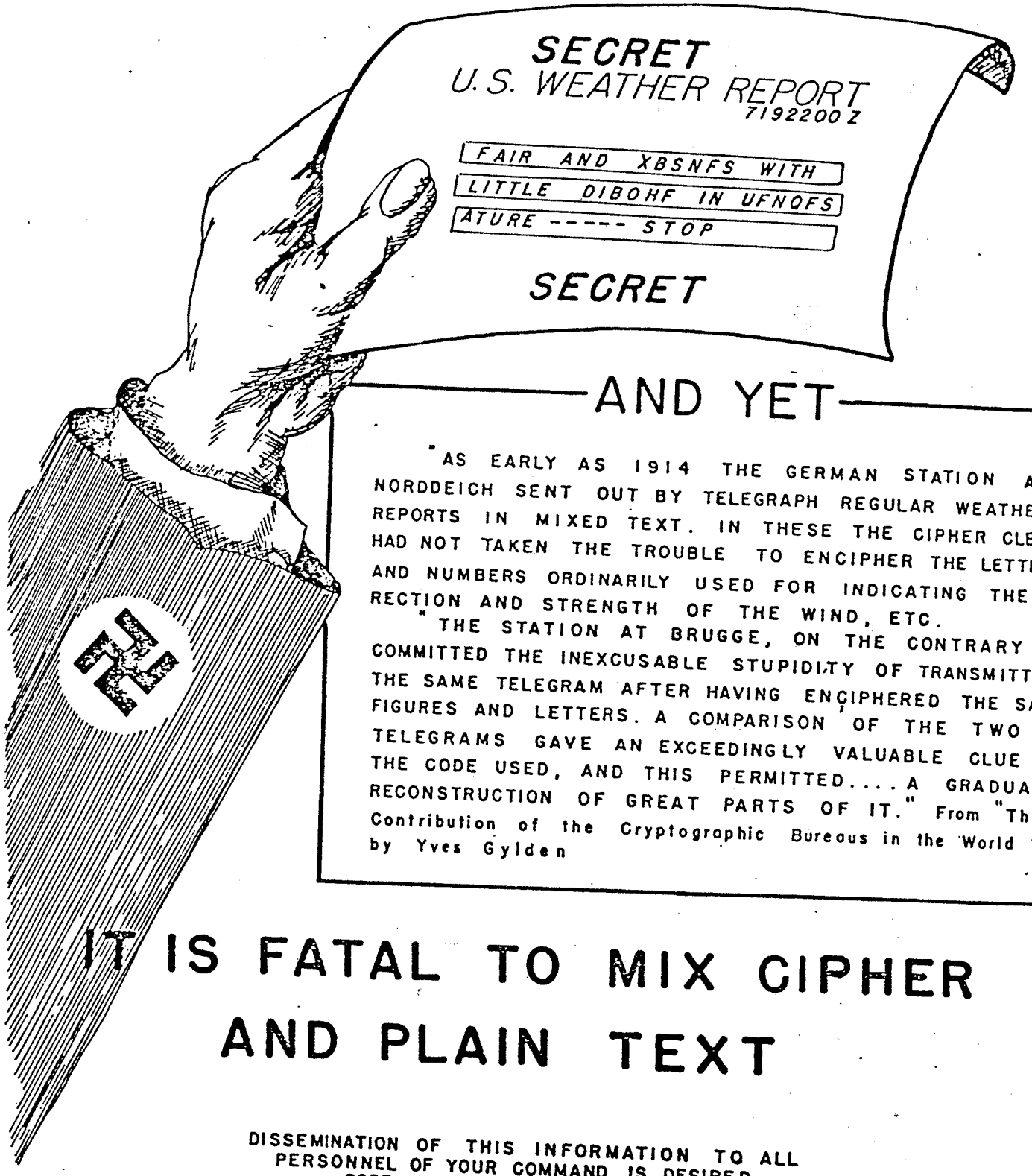
THEREFORE

NEVER REPEAT A CRYPTOGRAPHED MESSAGE IN A CODE OR CIPHER SYSTEM OTHER THAN THAT IN WHICH IT WAS ORIGINALLY TRANSMITTED.

DISSEMINATION OF THIS INFORMATION TO ALL PERSONNEL OF YOUR COMMAND IS DESIRED.

Dec. 1942 No 50 SSBR OCSIGO 11-24-42

EASY TO GUESS, ISN'T IT?



AND YET

"AS EARLY AS 1914 THE GERMAN STATION AT NORDDEICH SENT OUT BY TELEGRAPH REGULAR WEATHER REPORTS IN MIXED TEXT. IN THESE THE CIPHER CLERKS HAD NOT TAKEN THE TROUBLE TO ENCIPHER THE LETTERS AND NUMBERS ORDINARILY USED FOR INDICATING THE DIRECTION AND STRENGTH OF THE WIND, ETC.

"THE STATION AT BRUGGE, ON THE CONTRARY, COMMITTED THE INEXCUSABLE STUPIDITY OF TRANSMITTING THE SAME TELEGRAM AFTER HAVING ENCIPHERED THE SAID FIGURES AND LETTERS. A COMPARISON OF THE TWO TELEGRAMS GAVE AN EXCEEDINGLY VALUABLE CLUE TO THE CODE USED, AND THIS PERMITTED....A GRADUAL RECONSTRUCTION OF GREAT PARTS OF IT." From "The Contribution of the Cryptographic Bureaus in the World War" by Yves Gylden

IT IS FATAL TO MIX CIPHER AND PLAIN TEXT

DISSEMINATION OF THIS INFORMATION TO ALL PERSONNEL OF YOUR COMMAND IS DESIRED
SSBR OCSIGO 1 SEPTEMBER 1943

THIS IS YOUR DUTY

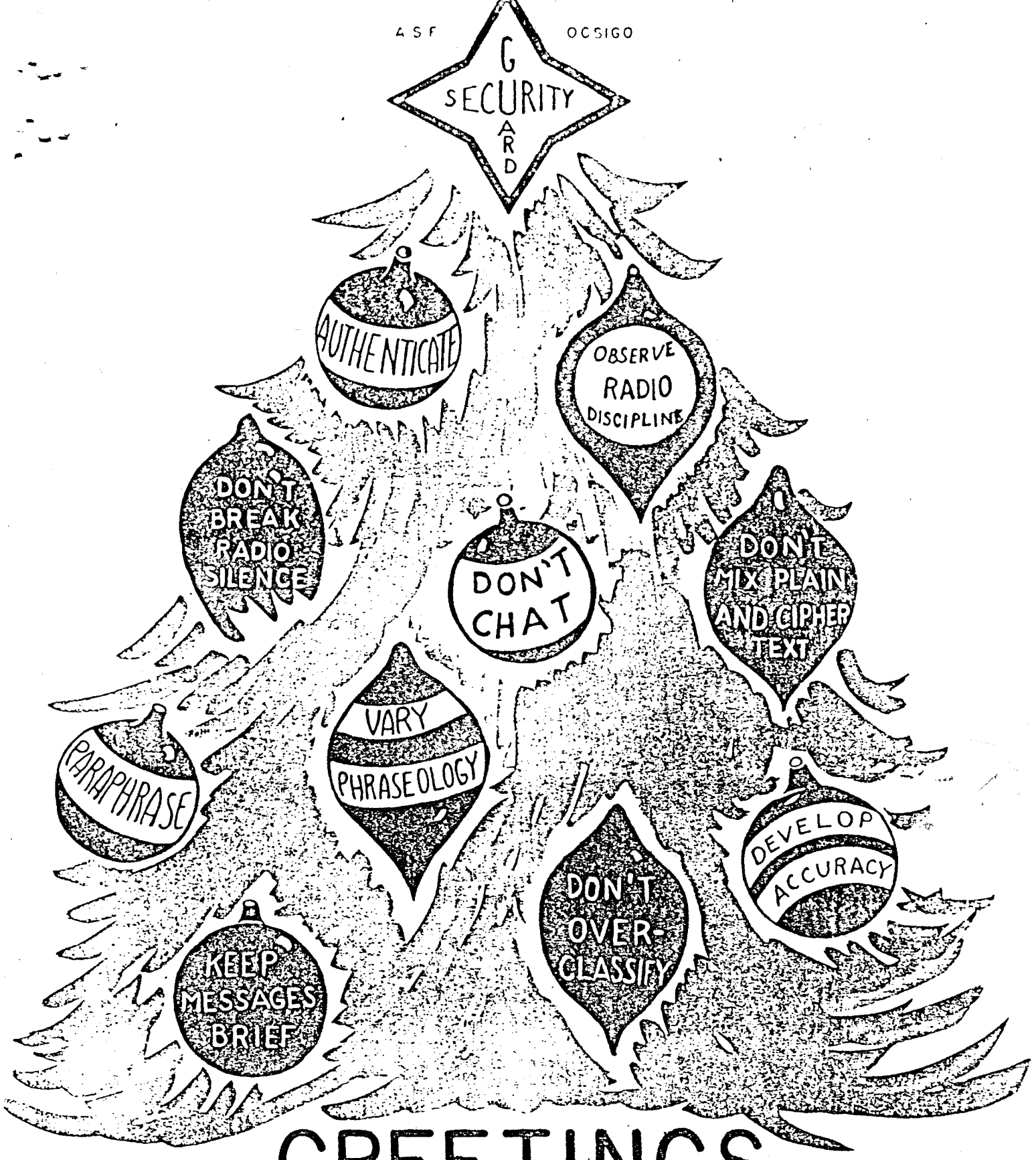
GUARD

CLASSIFIED MATERIAL FROM ALL UNAUTHORIZED PERSONNEL

DISSEMINATION OF THIS INFORMATION TO ALL PERSONNEL OF YOUR COMMAND IS DESIRED
SSBR OCSIGO 15 NOVEMBER 1943

No 39

ES

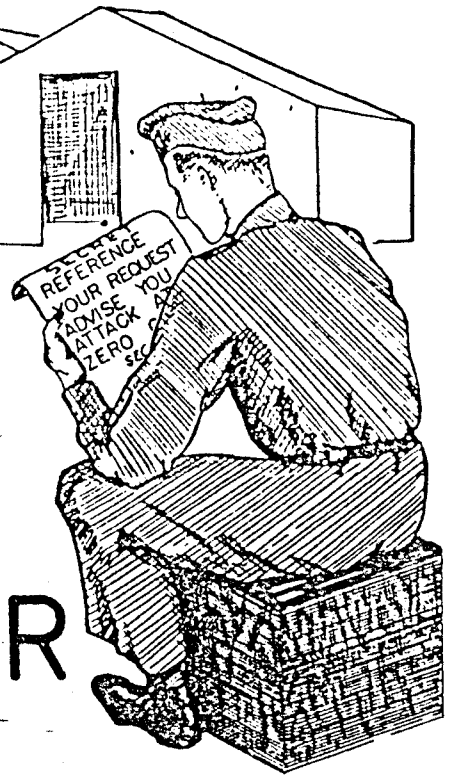


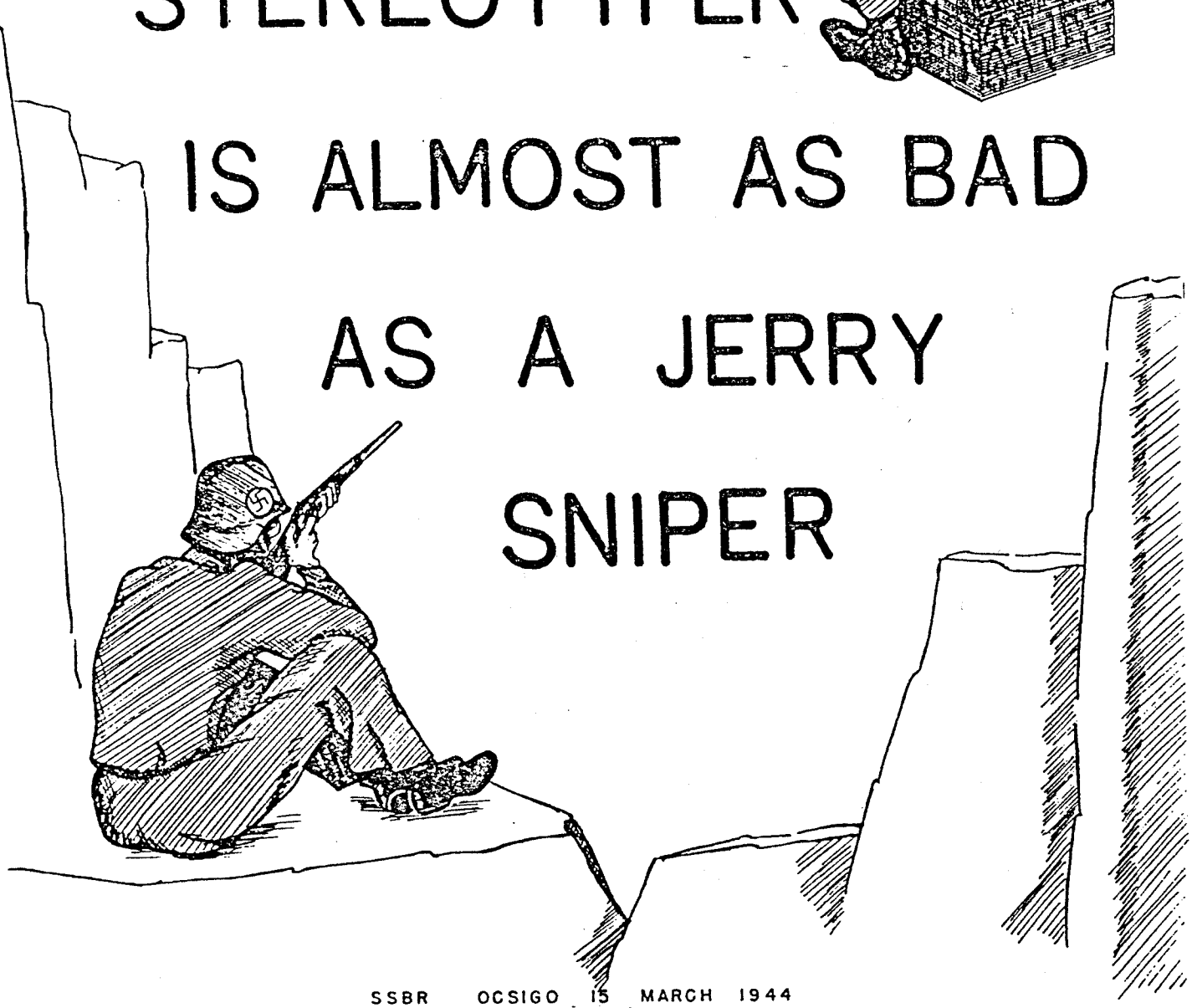
GREETINGS

START THE NEW YEAR RIGHT

DISSEMINATION OF THIS INFORMATION TO ALL PERSONNEL OF YOUR COMMAND IS DESIRED
SSBR OCSIGO 1 DECEMBER 1943

A GUY WHO'S A REGULAR STEREOTYPER IS ALMOST AS BAD AS A JERRY SNIPER



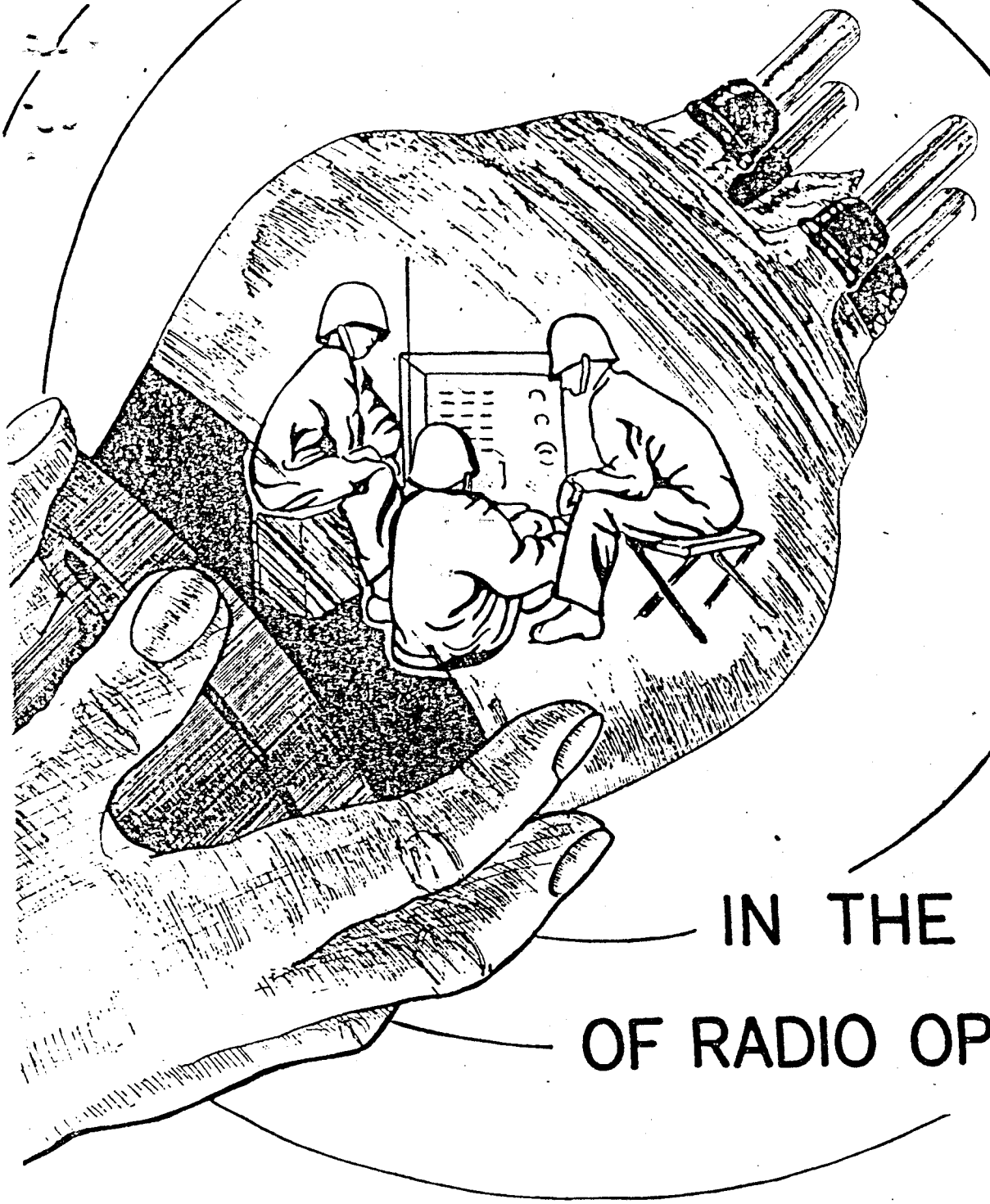


SSBR OCSIGO 15 MARCH 1944

43

E7

RADIO SECURITY IS



IN THE HANDS

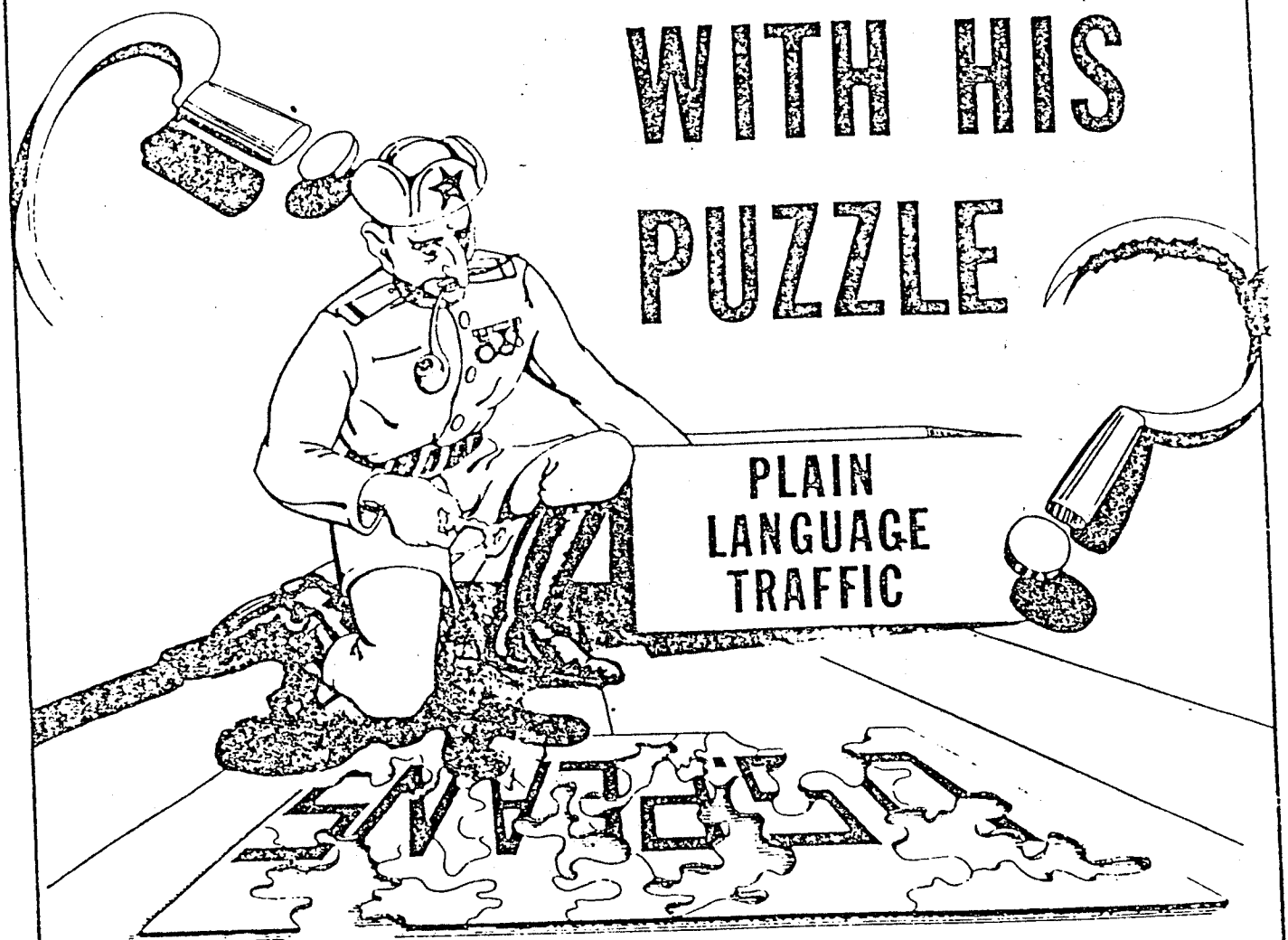
OF RADIO OPERATORS

Protect our troop movements, dispositions, and locations by observing prescribed radio procedure and maintaining circuit discipline.

SSBR OCSIGO 15 JANUARY 1944

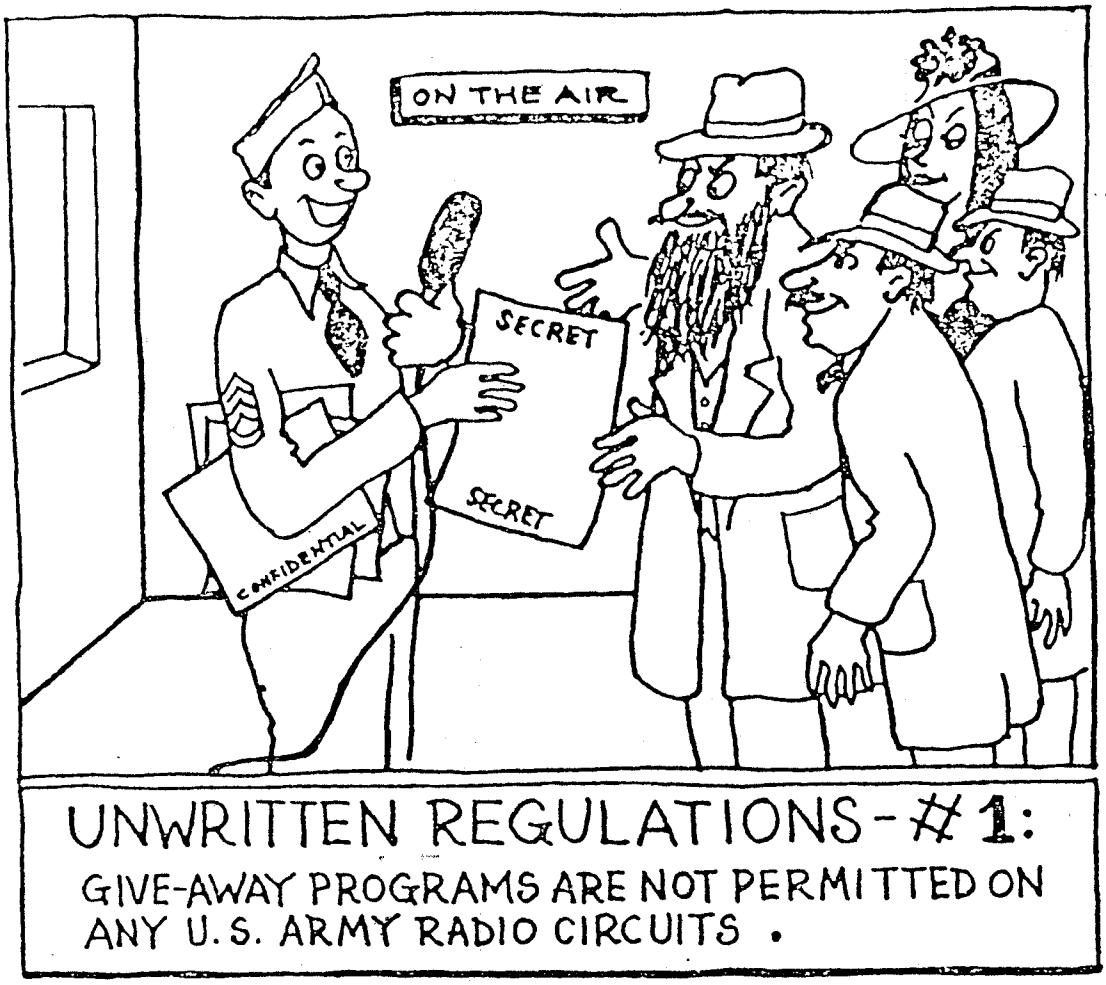
E 8

ARE YOU HELPING HIM WITH HIS PUZZLE



E9

Post WW II



UNWRITTEN REGULATIONS - #1:
GIVE-AWAY PROGRAMS ARE NOT PERMITTED ON ANY U.S. ARMY RADIO CIRCUITS.

"IT'S WORKING OK SO FAR, AND THERE'S BEEN A BIG DROP IN HUMAN ERROR."

E10

Korean War Period

"HOWDY FOLKS, THIS IS OL' TEX. FUNNY THING HAPPENED TO ME ON MY WAY TO THE STUDIO ..."

UNWRITTEN REGULATIONS -

#2: HOOPER RATING CREDITS MAY NOT BE OBTAINED ON U.S. ARMY RADIO CIRCUITS.

Korean War Period

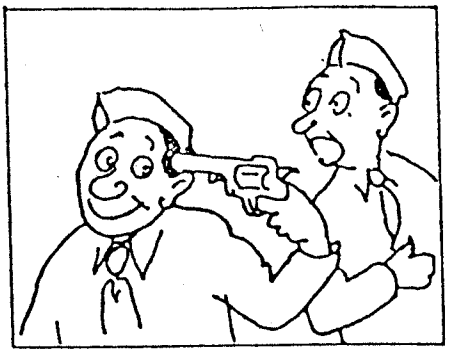
"THIS IS THE C.O. OF THE IFTHFAY ATTALIONBAY. WE ARE GOING TO LAUNCH A YOU-KNOW-WHAT AT DAWN TOMORROW."

UNWRITTEN REGULATIONS

#3: INVENT AS MANY SPECIAL SECURITY SCHEMES AS YOU LIKE, BUT DO NOT USE THEM UNTIL THEY ARE APPROVED BY PROPER AUTHORITY.

Korean War Po

TWO DEFINITIONS OF RUSSIAN ROULETTE



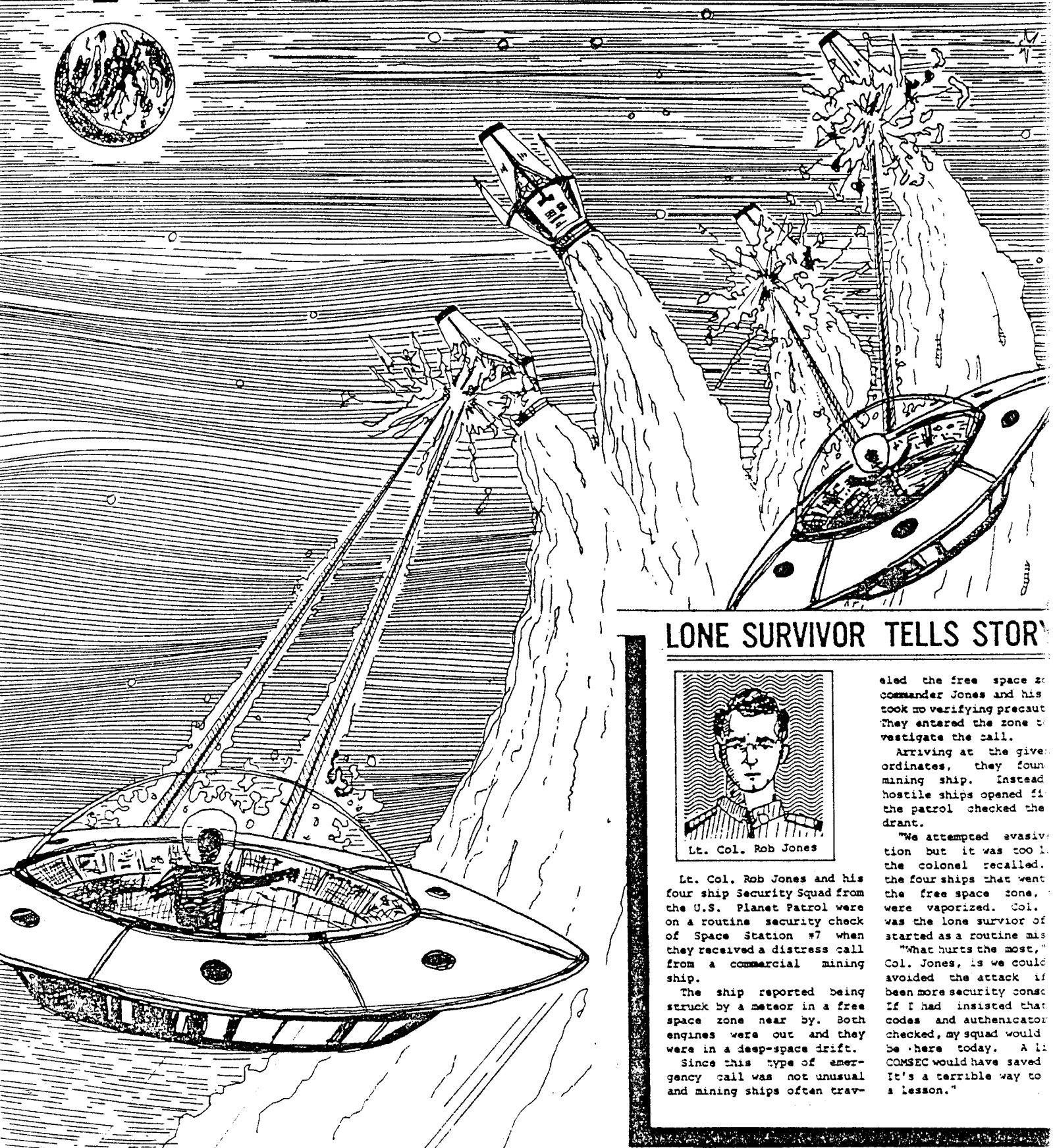
1. A GAME OF CHANCE USING A REVOLVER HAVING ONE LOADED AND FIVE EMPTY CHAMBERS. PLAYER ASSUMES HE WON'T BLOW HIS HEAD OFF.
2. A GAME OF CHANCE USING A TRANSMITTER AND CLASSIFIED INFORMATION. PLAYER ASSUMES HE WON'T BE INTERCEPTED.

UNWRITTEN REGULATIONS

#4: IF YOU DON'T HAVE TO TEST, DON'T. IF YOU DO, DO IT, BUT BE SURE YOU KNOW WHEN TO QUIT.

Korean War Period

U.S. PLANET PATROL AMBUSHED!!!



LONE SURVIVOR TELLS STOR

Lt. Col. Rob Jones

Lt. Col. Rob Jones and his four ship Security Squad from the U.S. Planet Patrol were on a routine security check of Space Station #7 when they received a distress call from a commercial mining ship.

The ship reported being struck by a meteor in a free space zone near by. Both engines were out and they were in a deep-space drift.

Since this type of emergency call was not unusual and mining ships often trav-

eled the free space z
commander Jones and his
took no verifying precaut
They entered the zone t
vestigate the call.

Arriving at the give
ordinates, they foun
mining ship. Instead
hostile ships opened fi
the patrol checked the
drant.

"We attempted evasiv
tion but it was too l
the colonel recalled.
the four ships that went
the free space zone,
were vaporized. Col.
was the lone survior of
started as a routine mis

"What hurts the most,"
Col. Jones, is we could
avoided the attack if
been more security consc
If I had insisted that
codes and authenicator
checked, my squad would
be here today. A li
COMSEC would have saved
It's a terrible way to
a lesson."

Without COMSEC there may not be a future.

THE TYPICAL COMSEC VIOLATOR COULD BE YOU!

Can you guess how our military opponents get the best and most reliable intelligence information?

They listen in on the typical COMSEC violator. It could be a friend or someone working in your office. Or it could be the supply clerk, the pilot, the maintenance specialist or... YOU!

Would you believe by listening to our communications?

You find this hard to believe? The following historical moment shows how good and bad communications security practices can even affect the outcome of battles.

BEN SUE, SOUTH VIETNAM DECEMBER 1969

One of the most startling discoveries during the Southeast Asia Conflict occurs in December 1969 near Ben Sue, South Vietnam.

While leading an assault operation on suspected Viet Cong locations, an Army Kit Carson scout notices a whip antenna in a bush. The antenna wire leads to a nearby tunnel.

Further investigation results in a quick skirmish that leaves one Viet Cong dead. Underneath the dead VC, the scout locates 12 other enemy soldiers huddled in an underground communications intercept site. He talks them into surrendering.

This marks the first time that a virtually complete unit with all of its equipment has been captured.

The unit, called Alpha Three, confirms long-held suspicions that the enemy monitors Allied communications and uses English linguists to misdirect artillery and air strikes against Allied troops.

All equipment captured was high quality and in excellent operating condition. With the equipment, the unit could listen to most insecure voice and manual Morse communications used by Allied tactical units.

Many captured documents revealed the enemy intercept effort was effective in determining air-strike times and locations, unit positions and nighttime ambush patrol locations.

During the interrogation, the captured unit commander reveals that on a normal day his unit intercepted 10 significant messages. He added that US night ambush operations are frequently compromised 24 hours ahead of time.

In terms of American casualties, the scope of this compromise remains uncalculated.

SIX WAYS YOU CAN PROTECT COMMUNICATIONS

CONSIDER THE TOPIC

When communicating, consider the topic. If it is classified or of intelligence value, do not use the administrative insecure telephone.

DON'T COMPROMISE

If the other party is placing you in a compromising position and ignores your warnings not to discuss classified information on the telephone, hang up.

SECURE SYSTEMS

Use secure voice equipment or approved cryptosystems to pass classified information. Use secure facsimile facilities.

MESSAGES

Use messages. All AUTODIN messages are electronically encrypted before transmission.

GIVE YOUR NUMBER

When releasing messages, include your secure drop number. This gives the receiving party an opportunity to call you on AUTOSEVOCOM to discuss the subject.

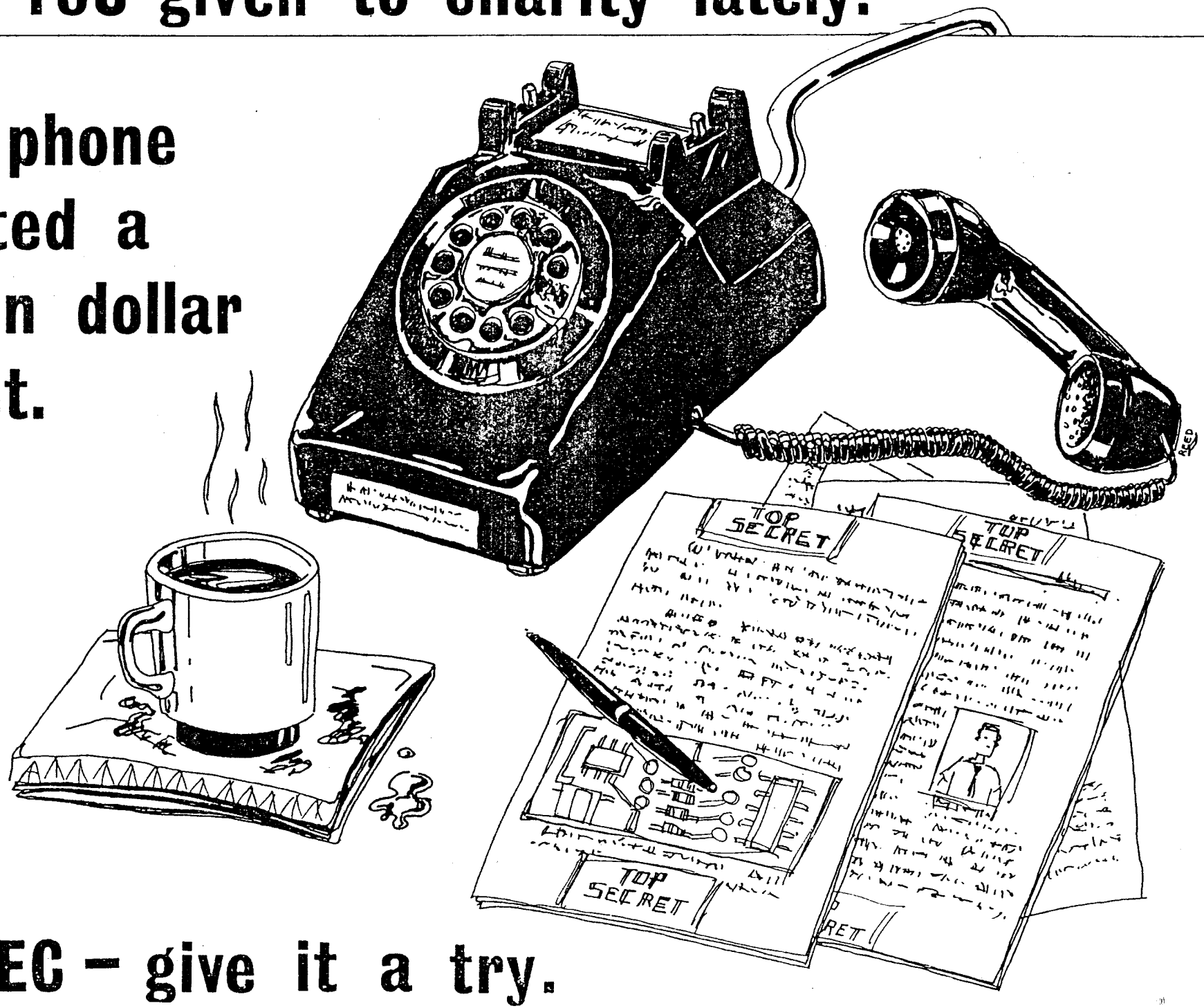
BE AWARE

Make sure that all personnel in your unit are aware of both the command's and unit's Essential Elements of Friendly Information, called EEFIs for short. EEFIs are bits and pieces of sensitive or classified information. The disclosure of this information might give a hostile intelligence operation the missing link needed to complete an intelligence picture.

DON'T BE TYPICAL!
PRACTICE COMMUNICATIONS SECURITY

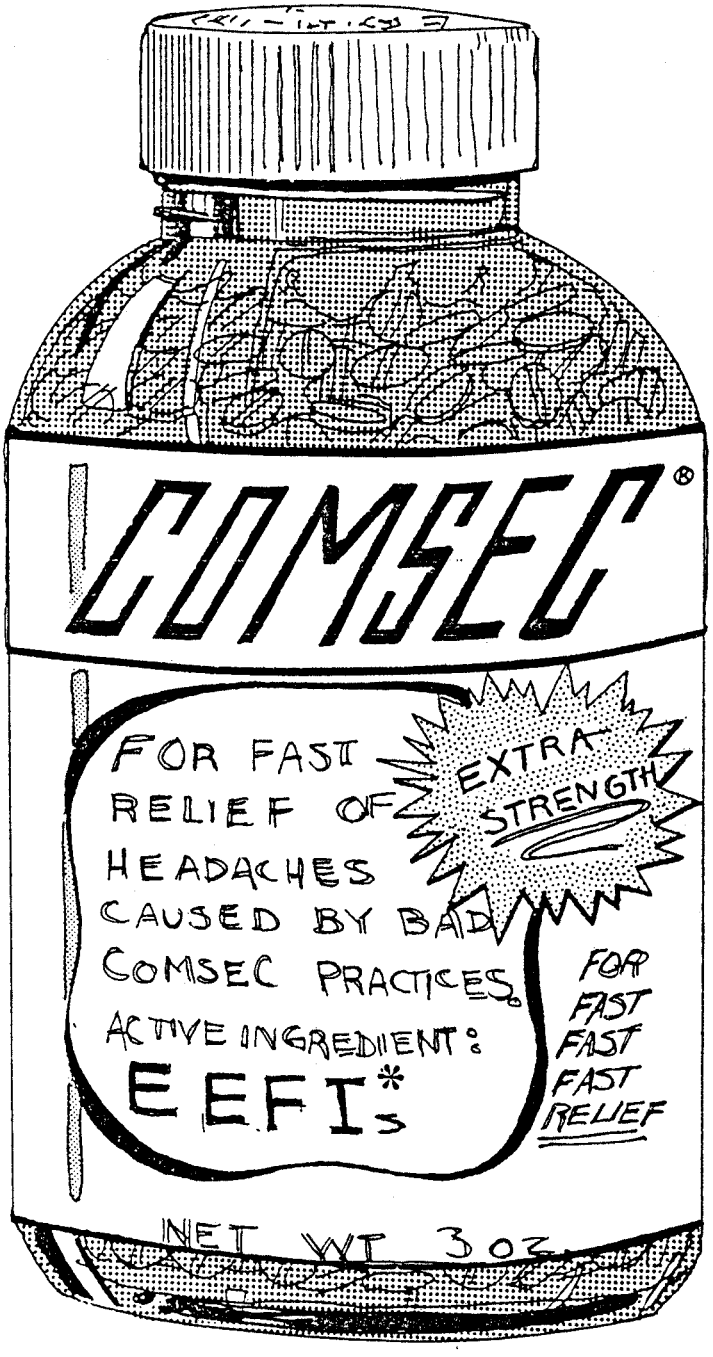
Have YOU given to charity lately?

This phone donated a million dollar secret.



COMSEC – give it a try.

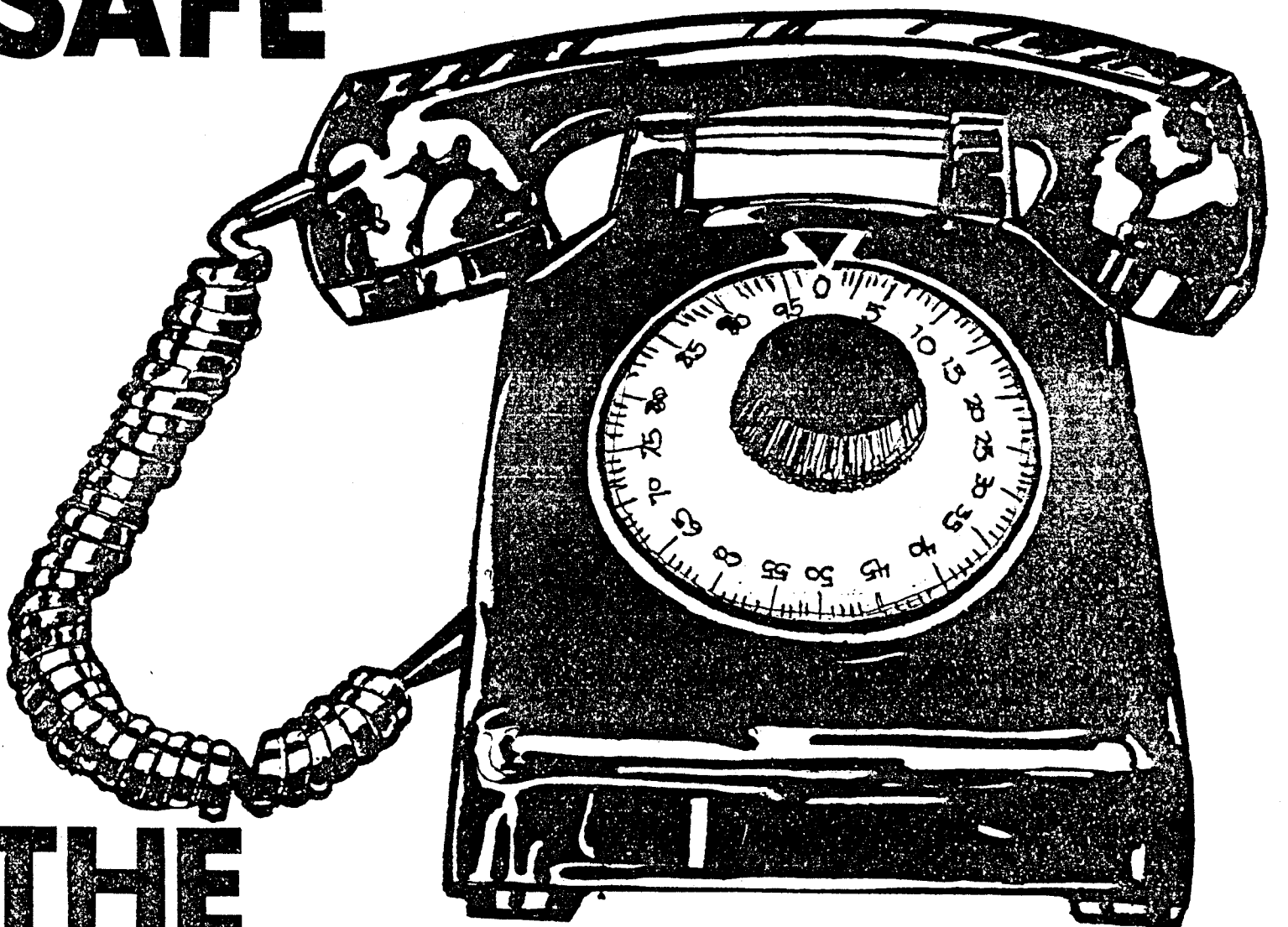
SECURITY HEADACHES?



TRY THIS.

* Essential Elements of Friendly Information

KEEP YOUR COMMUNICATIONS SAFE



THE COMBINATION - COMSEC & YOU

STOP MAKING THE INTELLIGENCE COLLECTOR'S JOB EASY...
KNOW YOUR EEFIs,

PRACTICE COMMUNICATIONS SECURITY.

DEFEND AGAINST THE

ENEMIES OF COMSEC!

YOUR MISSION:

DESTROY THE ENEMIES OF COMSEC
AND SPELL S-E-C-U-R-I-T-Y

OPEN PHONES — S
TRAPPED BY TIME — E
AWE OF RANK — C
TALK AROUND — U
FLAG WORDS — R
HOMEMADE CODES — I
UNCLASSIFIED GOSSIP — T
EMOTIONAL HAZARD — Y

PLAY TO WIN!!!