TOP SECRET

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

3rd Issue, 1987

P.L. 86-36

THIS DOCUMENT CONTAINS CODEWORD MATERIAL

TOP SECRET

CLASSIFIED BY NSA/CSSM 123-2
DECLASSIFY ON: Originating
Agency's Determination Required

NOT RELEASABLE TO CONTRACTORS

THE 200th ANNIVERSARY

P.L. 86-36

The bicentennial of the Constitution is an occasion
for celebration. We rejoice in its sturdiness and
flexibility. It is also an occasion for contemplation.
This elegant document is as much the result of a
bureacratic process, of negotiation and
compromise, as of philosophy.

Thanks to the media, – radio, TV, magazines,
newspapers – who provided "daily coverage" this
summer as if it were 200 years ago, we were able to
observe this process. The key issue then was the
power of the central government. We know this not
from an m/r attached to the document, but from the
minutes, letters, and notes of the delegates. We
know, too, that many delegates who participated in
this process foresaw that certain compromises were
bound to have unhappy consequences for the
country some time in the future. But they voted as
they did, albeit reluctantly, because they believed
that it would be worse for the nation not to.

The key constitutional issue in 1987 is the balanced
budget amendment. In commemoration of the
bicentennial, we present an essay on this subject by
an NSAer. His views, as you will see, are in part
shaped by philosophy, and in part derived from
first-hand experience with the bureaucratic
process.

We the People The Constitution

The national commemoration of the bicentennial of the U.S. Constitution has evoked considerable study and reflection on this great document and the ordered scheme of government it provides. Thus, there is no small irony in the fundamental misperception of the role and purpose of the Constitution displayed by supporters of a balanced budget amendment.

The U.S. Constitution was the product of an effort that found its original purpose in the need to alter the existing Articles of Confederation to provide for a more stable and effective form of government for the newly independent, loosely united former colonies of Great Britain. The demonstrable defects in the Articles of Confederation led the convention assembled in the summer of 1787 to produce a new governmental charter that allocated power between the newly created branches of the national government, redefined the distribution of power between the national and state governments, and established certain limits on the exercise of governmental authority with regard to the national constituency - the people themselves. The subsequent amendments to the Constitution have served as refinements to this basic organizational scheme without disrupting the principal purpose of the document: to allocate the division of power among the federal government components, the states, and the people.

In considering the call for a constitutional amendment mandating a balanced budget, the question arises as to what constitutional defect or omission requires this remedy. Is there a fundamental flaw in the governmental allocation of power that has produced this national fiscal crisis? Is the problem linked to a misalignment between the authorities conferred on the government and the rights reserved to the people?

The answer to both these questions is, of course, emphatically in the negative. Article I of the Constitution provides the Congress with all requisite authority to conduct and manage the fiscal affairs of the national government. The powers conferred in this Article represent a marked departure from the authority provided in the Articles of Confederation in recognition that the national government must necessarily be imbued with unconfined authority in respect to all those objects which are entrusted to its management.

What then is the purpose of a constitutionally mandated balance budget? Stripped of surrounding rhetoric, the purpose is simply one of imposing some sort of constitutionally based wisdom on the prudence with which Congress exercises its fiscal powers. "Wisdom" is of course an abstract term

susceptible of varied interpretations: what appears wise at one moment may seem foolish the next. Whether or not Congress is collectively exhibiting the requisite "wisdom" in exercising its fiscal powers is a function of the legislative prudence of its individual members.

Indisputably, Congress has all the necessary authority to produce a balanced budget now, without need for any constitutional tinkering. Its failure to do so is not the product of any constitutional deficiency; it is the result of a continuing series of collective legislative judgments on the exercise of Congress' fiscal authority. If those judgments are now seen as imprudent, the Constitution already provides the remedy: popular election of the congressional membership.

Advocates of a balanced budget amendment apparently misunderstand the role the Constitution plays in the performance of government. The Framers' intent was to ensure that the national government was provided with the means necessary to accomplish the ends entrusted to it. The wisdom with which any particular Congress exercises its constitutionally conferred powers is not a constitutional issue; it is a political one. Before the quintessentially political issue of proper fiscal policy is misguidedly framed as a constitutional one, all parties would be wise to recall Alexander Hamilton's admonition in Federalist No. 25:

> Wise politicians will be cautious about fettering the government with restrictions that cannot be observed, because they know that every breach of the fundamental laws, though dictated by necessity, impairs that sacred reverence which ought to be maintained in the breast of rulers towards the constitution of a country, and forms a precedent for other breaches where the same plea of necessity does not exist, or is less urgent and palpable.

In drafting the Constitution, the Framers wisely avoided shortsighted "fixes" designed to remedy problems endemic to their time because they realized they were creating a covenant that was to endure through the changing times of the future. Similar prudence should be exhibited now if we are retain any hope that the Constitution as we know it is to survive to its tricentennial. □

GOLDEN OLDIE

ARLINGTON HALL, c1955
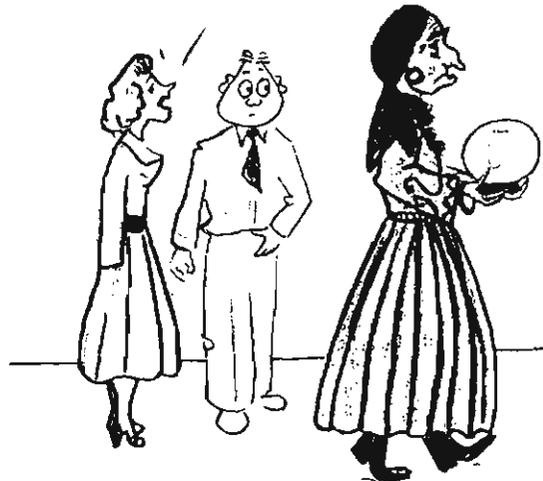
SHE'S CRACKED TWO SYSTEMS ALREADY!

---

g62
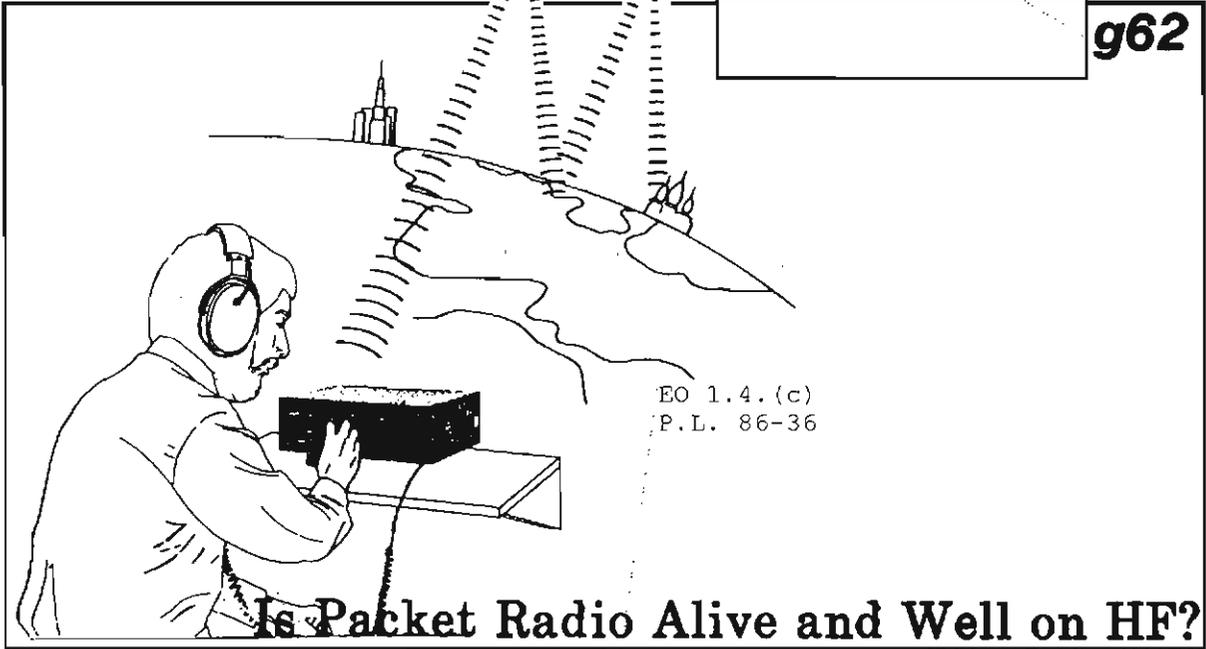
EO 1.4.(c)
P.L. 86-36

Is Packet Radio Alive and Well on HF?

accuracy is a must, this is not too high a price to pay.
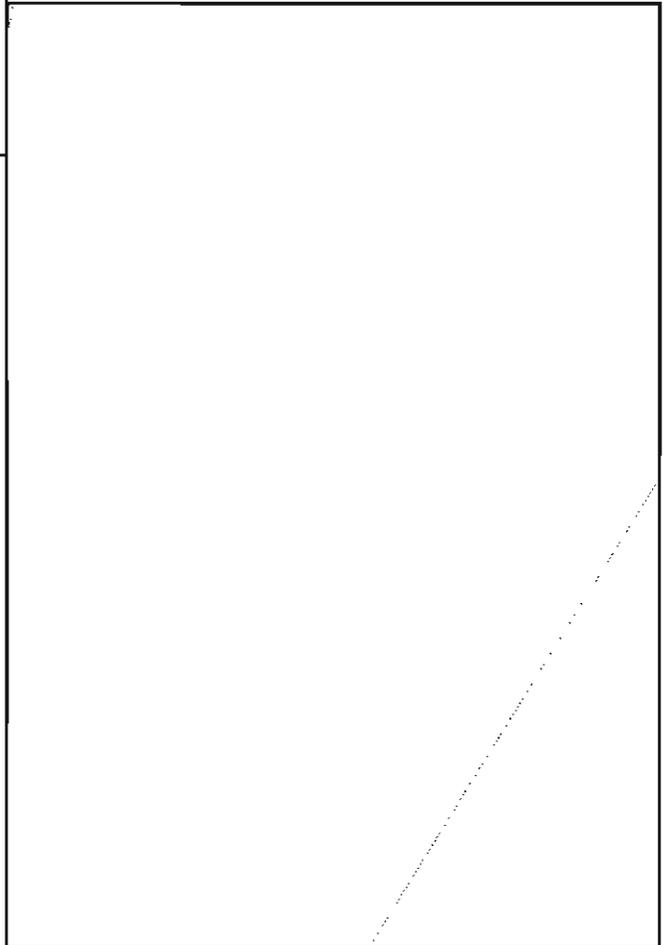
(U)   Packet is inexpensive! Figure 1 lists, as of August 1986, several terminal node controllers (TNCs) which are available to anyone. (Is the only market the amateur – the ham – radio operators?) These TNCs are the link between the only two other components needed for a packet system – almost any computer and almost any radio capable of transmitting voice communications. Not only are these units inexpensive, they are seemingly exempt from export controls, as anyone can buy one with no questions asked, simply by paying. You don't even to show the salesman your amateur radio license.

(FOUO) Packet is error-free! According to the AX.25 protocol, packet can, in theory, provide virtually error-free communications. In actuality, an error may slip in every few years! Although the transmission speed common in amateur radio circles is 300 baud on HF (1200 baud on VHF and above, and 2400 is being experimented with) the actual speed is considerably less. In many applications where

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

EO 1.4.(c)
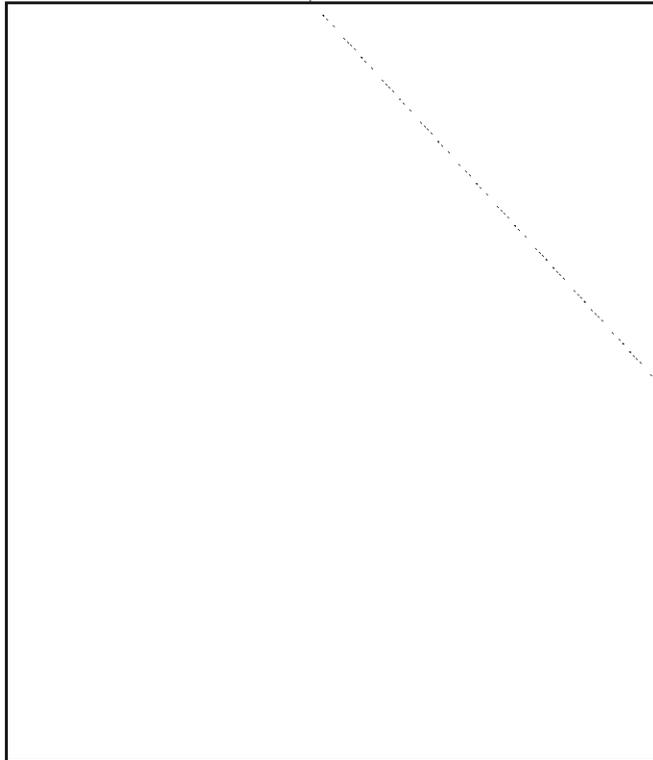
	Countries or Regions with Amateur Radio Packet Operations
	Argentina
	Australia
	Austria
	Belgium
	Brazil
	Canada
	Cayman Islands
	Chile
	Colombia
	Costa Rica
	Denmark
	Dominican Republic
	Ecuador
	England, U.K
	Finland
	France
	Greenland
	Guatemala
	Guernsey Islands, U.K.
	Haiti
	Hungary
	Indonesia
	Italy
	Japan

(U)   This operation would be very similar to telephone bulletin board systems for owners of home computers. This sort of operation is being done everyday by ham radio operators. As a matter of fact, the amateur radio operator community has developed packet operation – file (message) up/downloading, store and forward message handling, dual-port (i.e., "in" on VHF or UHF and "out" on HF or vice versa) operation. A side benefit of this type of communications would be reduced training for military radio operators, eliminating the need for 5 to 10 weeks of morse code training. Additionally, much of packet technology is available in open-source materials and is documented in many ham radio journals.

Jersey Islands, U.K
Kiribati
Kuwait
Luxembourg
Mexico
Montserrat
Morocco
Netherlands
Netherlands Antilles
New Zealand
Nicaragua
Northern Ireland, U.K.
Norway
Panama
Philippines
Portugal
Scotland, U.K.
Singapore
South Africa
Spain
Sudan
Swaziland
Sweden
Switzerland
Tanzania
Togo
United States
Vanuatu
Venezuela
Wales, U.K.
West Germany
West Malaysia/Sabah/Sarawak

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

FIGURE 2

P16

P.L. 86-36

BIG LOOK

⇒Since this article does not lend itself to portion marking, it is classified TSC in its entirety.⇐

During the Vietnam War, SIGINT elements in the Vietnam area were tasked with identifying and locating sites from which the North Vietnamese were destroying US aircraft with Surface-to-Air Missiles (SAMs). The following is a sketch from memory of the US Navy approach to solving the problem.

Working separately, COMINT elements were able to follow North Vietnamese tracking of US aircraft, and succeeded in intercepting readiness and firing commands so they could not locate the site that was preparing to fire quickly enough to destroy it. The usual analytic methods to determine position did not work because the Vietnamese moved missiles and crews from site to site overnight, as often as three or more times per week. Meanwhile, the ELINT elements were able to locate the FANSONG radars, but they had no way of knowing which SAM site they supported, or whether the operation was calibration, practice, or launch preparation.

The problem became acute when the Soviet advisors and the North Vietnames missile crews modified their procedures so that instead of tuning and calibrating their FANSONG radars at normal power, they used very low power, coming up to normal power only when a designated target was passed on to them to track and destroy. Thus our ELINT elements had no time to locate the FANSONG before a missile was already on the way.

At about that time, (early 1960's) electronic engineers attached to Fleet Air Reconnaissance Squadron One (VQ-1) devised two independent radar intercept systems, BIG LOOK and BRIGAND, that greatly improved our ability to locate radars. Used together, they were to help us solve the problem. The two systems were mounted in a modified EC121 airframe and sent to Danang, South Vietnam, for a trial. It proved successful enough to warrant expansion of the effort. At its peak, the effort provided continuous coverage whenever US strikes were made in the Eastern part of North Vietnam, using four platform aircraft and some 100 crew members each day.

The project itself was given the covername BIG LOOK. It was assigned the mission of interception, identification, and location of North Vietnamese SAM emplacements as targets for strike elements, and of providing warning to those strike elements of impending launches of missiles against them.

Development of the BIG LOOK equipment made it possible for ELINT evaluators to get a position

on the FANSONG radar before it was up in the tracking mode and able to endanger US strike aircraft. BRIGAND was tricky to work with, but its capability to lock onto the rotation of a radar such as SPOON REST and position it with an accuracy sufficient to strike it after only one successful intercept made it worth all of the problems it engendered.

The primary problem was calibrating BRIGAND to the tolerances necessary to provide accurate fixes. Unfortunately, that accuracy was achieved only occasionally. A second problem was the high power requirement for both BRIGAND and BIG LOOK. Overheated wiring was very common, and it was not unusual for a platform to have several electrical fires while
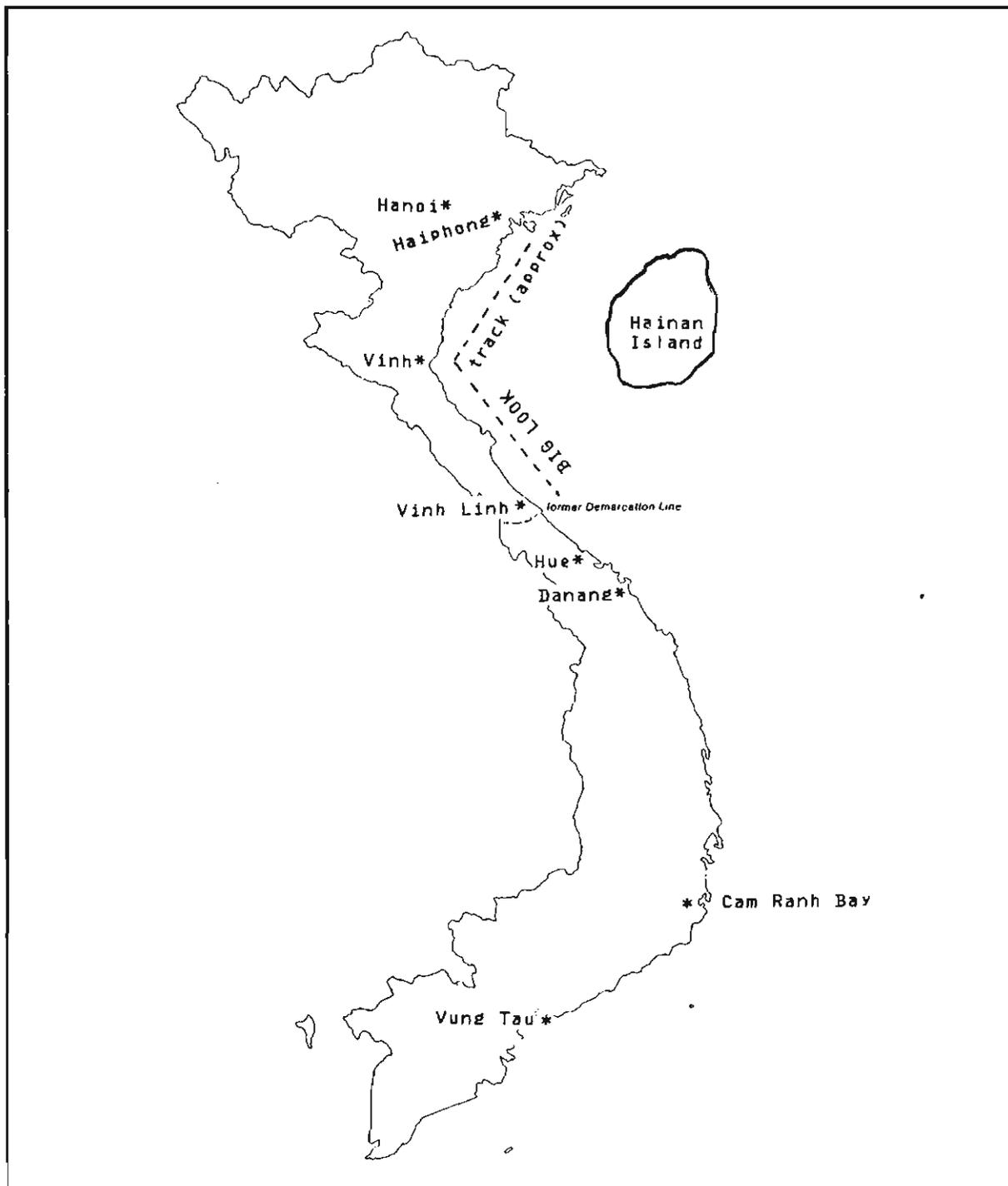
EXPLANATORY NOTES

BIG LOOK. US radar intercept receiver coupled to an antenna with an oversized reflector, giving the system enough sensitivity to detect a radar emitting at very low power.

BRIGAND. US radar intercept receiver modified to have the ability to lock onto the sweep of a target radar and to present an offset representation of the return of the target radar.

DUMMY LOAD. Mode used used by the Viet Cong (or Soviet advisors) in warming up and calibrating the FANSONG radar to avoid detection until it initiated actual target tracking/missile guidance operation.

EC121M. The BIGLOOK platform aircraft. A modification of the C121, also known as the Lockheed Constellation.

FANSONG. Target tracking and missile guidance radar for the Soviet SA-2 missile that was widely used in Viet Nam.

SPOON REST. An air search radar used by North Vietnamese air defense forces.

airborne during any one deployment. A third problem was training ELINT evaluators to the level required to make accurate fixes, and keeping them on after they attained that experience.

The ELINT side of BIG LOOK was composed of BIG LOOK and BRIGAND. The COMINT side had four voice and two morse intercept operators, along with a teletype operator and the COMINT evaluator. The COMINT detachment officer in charge, Vietnamese linguists, and some others were drawn from USN-27 at San Miguel,

All were detailed for periods of three to six months to VQ-1, until late in 1968, when they were detailed to the Navy COMINT actvity at Danang. The aircraft, flight, and ELINT crews were drawn from VQ-1 elements at the for a deployment period nominally of six weeks.

Intelligence support to BIG LOOK included US strike schedules which were received on a daily basis and briefed to aircrews before takeoff. On-board secure teletype provided schedule changes or additions. This permitted the COMINT evaluator to concentrate attention to scheduled air strikes.

Flights were eight hours long. One hour was allowed on each end for transit from Danang to home station and return. Most flights were conducted at five thousand feet above and parallel to, and some ten to fifteen miles to seaward of, the North Vietnamese coast between about 17°30' North and 20°15' North (or, between Vinh Linh and Nam Binh, North Vietnam).

Once airborne, the COMINT evaluator was passed morse and voice intercept of North Vietnamese air defense tracking of strike aircraft, and was alerted by voice operators who were listening to the air defense voice net when a missile launch was imminent. Then the COMINT evaluator alerted the warning officer, who coordinated with the ELINT evaluator to get a position on the FANSONG as soon as it began active tracking, and issued a voice warning to strike aircraft in the area. Interaction between COMINT and ELINT evaluators was necessary, since the ELINT side could provide DF on a radar, and the COMINT side could follow readiness and intent. When the system worked, that is, when BIG LOOK intercepted a FANSONG as it came up in guidance mode just after a SAM site was ordered to fire, then a valid warning could be broadcast for that area. Warning was based on a US grid system that was defined into segments small enough to be useful, and yet simple to use and understand quickly.

After a flight was completed, all SIGINT was fused by the evaluators and analysts into a report designed to provide strike information to the strike forces and intelligence information to the community as a whole.

The strike pilots and the commanders of strike units were most appreciative for the warnings provided by the crew members of the airborne platforms. This gave them a great deal of job satisfaction, and somewhat offset the effects of conditions under which they performed their tasks. □

The Joys of US Government Travel

G53

This article is classified CONFIDENTIAL in its entirety because of the sites visited.

As many story tellers would say, Once upon a time there was a young man who at the age of 20 decided to join the Air Force. I was this young fellow and I had lived all of my life in West Virginia with only brief trips to the five surrounding states and the District of Columbia. My longest plane or train trip at that time had been between Washington, D.C. and Charleston, West Virginia. As a small-town boy, I was looking forward to some worldly travels in the Air Force.

My first trip was from Charleston, West Virginia to San Antonio, Texas with a number of stops in between. Had I been a bit wiser at that time, I would have suspected that my travel horoscope was on a very interesting track. This flight was not scheduled to be on the ground anywhere for more than a few minutes before arriving in Texas. But for this traveling novice and his new companions, there was a 15-hour delay in New Orleans where I was without money or a place to sleep: somehow our plane arrived too late to connect with the onward flight to Texas. At the age of twenty, the solution for this problem was simple - find a comfortable seat some place in the airport and call that my bed for the night.
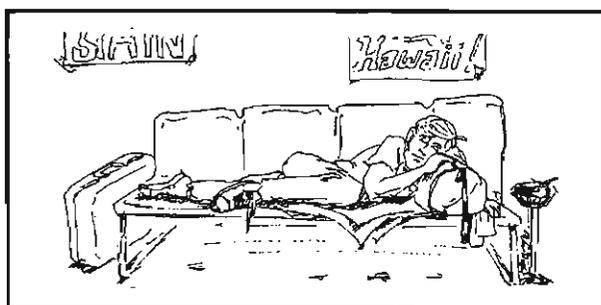
The next Air Force-sponsored trip was from Charleston, West Virginia to San Francisco, California. All was going well on this one-stop (Chicago) trip, when suddenly the plane lost cabin pressure over the Rocky Mountains,

within sight of Mt. Whitney. A number of older people on this flight experienced breathing problems; many blacked out from the lack of oxygen. The pilot of the aircraft immediately turned back from the mountains and "hit the deck" (went to a lower altitude). Breathing was considerably easier at the lower altitude, but many of the older passengers continued to have problems. We were met at the Albuquerque airport by a number of ambulances with their lights flashing. After dispatching several of the passengers and having some repairs made to the aircraft, we were once again on our way to San Francisco to meet an onward flight to Japan.

When returning to the US from Japan some eighteen months later, I was once again faced with a day-long (propeller driven aircraft) flight to the States. The first stop on this flight, Wake Island, was reached without difficulty. The second part of this trip found us midway between Wake Island and Hawaii in a storm. This storm was a real roller coaster which eventually cost us two engines on a four-engine aircraft. The pilot announced at that time that we were "past the point of no return," which I soon learned was a point where there wasn't enough fuel to return to Wake Island and that our only reachable destination was Hawaii. Again we hit the deck for a very slow and bumpy ride to Hawaii, where we were met by fire engines and ambulances.

I have been told that there is often something good in something bad; this stop in Hawaii was no exception. We were housed at no expense to ourselves at the Hawaiian Village Hotel for a week (just before Christmas) while personnel were brought in from California to fix this chartered aircraft. After repairs were made, our first attempt to continue our trip got us only to the end of the runway. More work on

the engines was necessary before we could head on to California.

To paint a little clearer picture of my situation at this time and how I was looking forward to getting home, I had been married only five months before going overseas for eighteeen months, I hadn't talked by phone to my wife throughout this period because of the cost, and it was nearing Christmas. All of this made me want to get home as quickly as possible. Come on, plane, let's go! The flight between Hawaii and California was generally uneventful until we were within sight of the West Coast. The pilot came on the intercom to announce that the plane had lost all of its hydraulic fluid and that the wing flaps, wheel release, and brakes would be affected by this situation. Further, he said that the runway at March Air Force Base was not long enough for our plane to land (with only mechanical brakes), so on to San Francisco we headed.

Yes, again we were met by fire engines and ambulances. And the landing was uneventful. By this time, however, I thought I had had enough flying for a while and decided to take a three-day train trip across the states, my longest train trip ever.
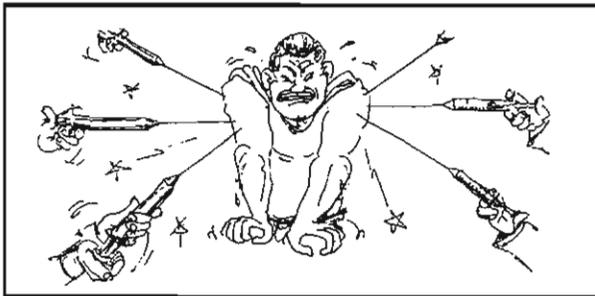
This was about it for the events I faced while in the Air Force, and next came my civilian trips for NSA. The first of these of any significance (meaning that there were several previous trips, mainly to Texas) took me to Vietnam. I was informed that I had to be ready to make this trip in just a matter of days, and that meant getting shots, passport, and whatever else was required prior to this time. Shots—I can still remember how my arms felt after "Buck Rogers" in the NSA dispensary got through with me, and then came the doctor with one for my hip pocket. Wow, that last one really felt good after I had been on that plane for over 24 hours; and my arms were so sore that I could hardly carry my

suitcase when I finally did arrive at Saigon. By that time, I was wondering how the fighting in Vietnam could be any more painful than just getting ready for this trip had been---in fact, I was beginning to wonder who the enemy really was.

I had made it, though, after a jet flight that took some 28 consecutive no-sleep hours to complete. This flight was generally okay except for having a slight delay in Guam waiting for fighting in/around Saigon to clear, having to fly on the edge of a typhoon just off the Philippines, and having to make a very strange landing in Saigon. The pilot informed us that he had to make a very high approach to the runway in Saigon in order to stay out of sniper fire range - my first real feeling that I was in an unfriendly place. The approach to the runway was high until we made a very steep descent; it worked, and there were no fire engines or ambulances there to meet us, either. (Only seconds later, however, as we were departing the plane, two planes collided on the runway as one was taking off and another was landing.)

My first night in Saigon was a real learning experience. Have you ever heard of being in a fighting zone and getting a room in a normal hotel? Well, that is what I did. I was informed that this hotel was okay, since it had "flower pots" in front of it---a sign that its dues had been paid to the bad guys and that it would not be attacked. I made my way to my room where I found three beds. I decided to wash several pieces of clothing at that time, and little did I know that the water was going to be red (rust) when I turned it on. My white clothes turned red at once, something that only the local Chinese laundry was able to correct. I also remember how this water situation forced me to buy soft drinks on base in order to have something to drink and for brushing my teeth. I climbed in bed later in the evening with a mind full of worry about my situation. Would I wake up if there was fighting during the night? What would I do, since I was by myself and knew nothing about this city? I couldn't fight, because I was unarmed (allowed only to wear fatigues and carry a Geneva Conference Card). How would I communicate with someone if I needed help, since I couldn't speak the language?

I did manage to get to sleep, only to be awakened by somebody walking around in my

room. I quickly jumped out of bed to find out who the intruder was. I learned that it was another American and that it was common practice in Vietnam for all three beds to be individually rented to different people. I really began wondering at that time who the third person would be, possibly a bad guy? Well, the night passed and morning came with no new person in the room. I was suprised, however, to learn on my way to work the next day that an attack had been made on Saigon during the night and that rockets had exploded only a few blocks from our hotel. I must have been tired, as I didn't hear a thing, and I missed my first battle.

Everybody's work day in Vietnam was long, and mine was no exception. Generally, it was seven days a week from 0430 to 2300. I subsequently made several trips throughout the country where I soon learned to use my flak jacket as a seat pillow on plane rides because any incoming fire would be coming up from the ground. I also learned not to be in any hurry (as the old military saying goes, "hurry up and wait") because military planes did not fly by set schedules. It didn't take long for me to realize that I should take advantage of every chance I could get to grab some zzzz's.

I spent several days during this TDY waiting for transportation in terminals which had nothing more than dirt floors, no roofs, and sometimes only two walls standing. Several interesting things occurred on this trip that I will never forget. One had to do with a well-known Air Force officer at Da Nang. I had made plans, after being in Vietnam for several weeks, to sleep a little late on one particular Saturday morning. Very early in the morning, however, this officer banged a pipe on the end of my bed to wake me. He said that this was a war zone and that nobody was allowed to sleep in; TDYers were no exception. He asked me to get dressed, and he proceeded to give me breakfast which he had gotten from who knows where. While eating, he told me that we were going to add another room to his operations area. This required our cutting a hole in the side of an existing Quonset hut with a torch and moving one end of a trailer into this new opening. My job was to hold the ladder while the officer cut the hole.

All was going as planned, when we heard someone inside yelling "Fire!" The officer stopped cutting at once, uttered a few

expletives, and ran around the building to discover that he had burned the tracking map to a cinder. Of course, the operations building was evacuated because of smoke, but officially it was because of hostile conditions, not further specified.

Another time, in Pleiku, very soon after arriving in Vietnam, I found out that I had a yellow stripe down my back. I was staying in the VIP tent which was some distance from the other tents and right next to the bunker. I asked whether there were any enemy in the area, and I was told that they never attacked during the dry period and, boy, was it dry that day. I was really happy to hear this news, but later that night there was a very loud clap of thunder, and the sky opened. It rained so hard that the water was coming through the fabric of my tent.
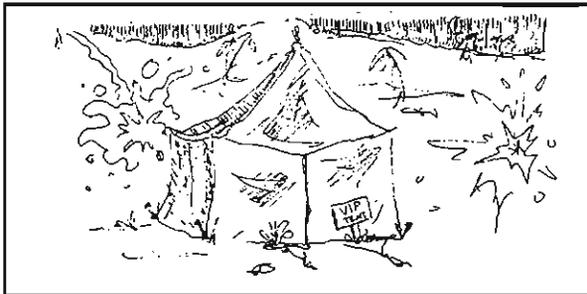
I started thinking about what I was told earlier that day about attacks, about the VIP sign in front of my tent being a good advertisement for attracting the bad guys; about the tent being off by itself where nobody could hear me even if I was in trouble, etc. I devised a scheme to wake myself should someone appear at my tent door: I put a wash pan next to the door, assuming that if anybody opened the door, it would knock over the pan, and the noise would wake me. I placed my shoes at the foot of my bed with my helmet between my shoes, thinking this surely would make for a quick exit if I had to leave. Sleep, yes, sleep; I thought I was finally going to get some sleep.

Clang! The pan fell, and I was gone like a flash. But nobody was there. I wondered where the enemy was. Evidently the wind had blown the door open and knocked over the pan. I decided if that alarm system wouldn't work, I would just zip up the front of the tent. But then I realized that if someone put an explosive under the wall of the tent I would be dead before I could get the door open to exit.

Finally, I decided to take my chances and just go to sleep. That I did.

I was surprised the next morning to learn that incoming rounds had destroyed two antennas only a few hundred feet from my tent. Would you believe that I slept through my second brush with war? Other excitement was on its way, and sooner than later. I learned not to worry about those things which were beyond my control, and I slept every chance I got.

My trip home, via Thailand, the Philippines, Okinawa, Japan, and Hawaii, was uneventful. I left Vietnam with blisters on the bottoms of my feet from the hot pavement and arrived in Baltimore where there was over a foot of snow on the ground. I waited outside the terminal in summer clothes for four hours before I was able to get a cab home...I nearly froze to death the remainder of that winter season. Also, I will add that my weight was 149 pounds when I started this trip and 129 pounds when I returned...mainly because of the lack of food and sleep (I averaged approximately four hours of sleep each day for the duration of this extended TDY). I also ended up with a fungus on one foot that continues to defy treatment to this day.

My next big journey was to [   ] My trip from Baltimore, via New York and [   ] was uneventful. After arriving [   ] we claimed our baggage, passed through customs, checked at the ticket counter about our travel reservations [   ] and proceeded to reenter the international area of the terminal. This part of the terminal was extremely crowded and noisy. After some two hours of waiting in this area, we realized that our flight was either on its way without us or that it was delayed. We weren't quite sure which was the case. We made a trip to the information booths where we found a representative of the airlines responsible for our flight [   ] We asked about our flight [   ] and were very pointedly instructed to see another person representing the airline responsible for taking [   ] This was annnoying, but, rather than make a scene, we decided to comply.

We walked around to the opposite side of the 15x20-foot information booth, and suddenly there was an explosion. My natural yellow streak reappeared, causing me to duck immediately, and I then attempted to determine
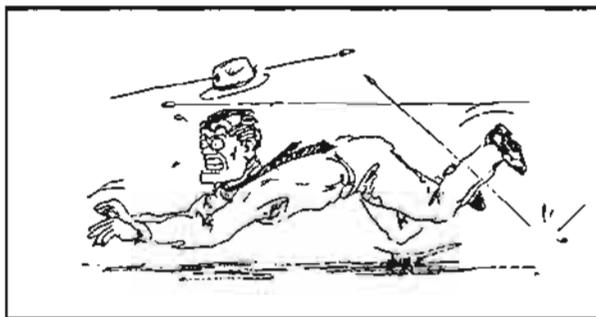
the cause of the bang. Much to my surprise, I saw another movement like someone throwing something on the opposite side of the information booth. I immediately hit the floor, and then heard another bang ringing through the building. Several more bangs sounded, followed by automatic weapons fire. I now know that the sound of ricocheting bullets as depicted in old western movies is realistic. They really do make such sounds as they glance off marble walls and glass windows.

The next thing I heard was some people talking on the other side of the information booth. Taking stock of my surroundings, I became aware of a woman and her husband not far from me. The woman was suffering from shrapnel injuries over most of her lower abdomen. Another woman was separated from her husband and was about to walk out in front of the terrorists. We were able to stop her before she made this mistake. Then there was a young girl who had it in her mind to jump through a very large plate glass window simply to get out of the building. With difficulty, two of us were able to hold her down until she regained her senses. We stayed on this floor for what seemed like an eternity, but it was probably less than 30 minutes.

My traveling companion asked me what I thought we should do and my answer was "I'd rather be most anywhere other than in this building right now---even the middle of the runway dodging airplanes would be better than where we are now." We decided to make an arm-in-arm chain (all of the people described earlier) and attempt to get out the nearest exit before someone saw us. This door was only 30 or so feet away, but the distance seemed endless as we ran for the door. Looking over toward the area of some yelling, I observed a number of people standing in a line with their hands up...forming a human barrier between the terrorists and the police. Later, I learned

CONFIDENTIAL

that the people standing next to me as I talked to the first person at the information booth were killed during this event...it was only a matter of seconds that kept me from being next to them when this occurred.

After we got out the door safely, we got the injured woman to an aid station. Then we were taken to another terminal, where we caught our plane[   ]we made another mistake. As we walked to dinner one evening, unknowingly we passed [   ][   ]something we learned from our hosts the next day was a real no-no. Although we encountered a number of hostile looks and were followed, we made this trip to and from our eating place without incident.

Four days after the airport incident, we were attempting to leave[   ]when suddenly, as we were traveling down the runway, there was a loud banging noise under the aircraft. The pilot immediately braked and returned to the terminal building. Several "mechanics" came on board the plane and started taking the floor apart. Several of these mechanics subsequently disappeared under the floor for a while, and one of them reappeared after a time. He disappeared from the plane, only to return with a large pry bar and a sledge hammer. Again he disappeared under the floor, and there was a lot of pounding taking place just below my seat. The mechanics reappeared after a while, and the floor was replaced. Another attempt was made [   ]and the exact same situation occurred again.

We returned to the terminal apron and waited three or four hours for another plane to be flown in from who knows where to take us to [   ]but of course we had already missed our flight[   ]We rebooked our flight, the last flight for the day[   ]and proceeded on our journey. Our stay[   ]was filled with new excitement.

While there, we were able to get a US Army helicopter flight that nearly ended in disaster. We were flying at 5500 feet when suddenly a gust of wind placed the aircraft on its side; a helicopter flies only one way in this position, down. The pilot was fighting to gain control of this bird, when suddenly it righted itself and

rolled over on its other side---down some more we went. By the time he was able to regain control of this craft, we were only 500 feet above the ground. Needless to say, I was a bit frightened by recent events and beginning to worry about what was going to happen next. In fact, I made the statement that I would like to have a rowboat to get home.

[   ]where one week later my traveling buddy and I became sick---food poisoning. After some recovery time, our next stop was[   ]where we were not allowed to depart the runway for several hours, because of a strike by aircraft controllers. From there, we made our way[   ]where one suitcase was virtually destroyed. Then we went on[   ]where we got a rent-a-car.

[   ]we suddenly realized that the transmission linkage on our rent-a-car was not working properly. We stopped the car and learned that a nylon ball and socket joint had worn out completely and would not stay together. After trying to get help from other passing motorists, we decided to do a real no-no again-[   ][   ][   ]and broke it just enough to make it fit the shape of the transmission linkage.
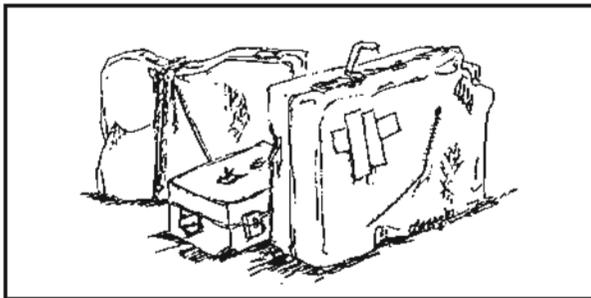
I learned one thing during this trip. If you are traveling overseas, you should always have a roll of nylon tape and a roll of toilet paper with you at all times. The domestic paper in these countries is ridiculous, and the tape allowed me to mend my broken suitcase and repair the transmission linkage. We made the rest of this trip uneventfully, until we arrived at Baltimore. My broken suitcase, from which I had removed all valuables, arrived as scheduled. My good suitcase, containing those valuables, was missing. I made the usual claim, and some two weeks later I recovered

CONFIDENTIAL

EO 1.4.(c)
~~CONFIDENTIAL~~ L. 86-36

the other piece of luggage. Fortunately, nothing was missing. However, there were tags on this suitcase from nearly every country in South America; and there was a carton of cigarettes and a box of candy in this suitcase which were not mine.

This travelog could continue for a while longer, but I believe you now have a feeling for how exciting government travel can be and what one federal employee has been through. I could tell you about the time that we were in a severe storm (with significant amounts of lightning, rain, and hail) over London---a storm so intense that it forced the pilot to make an emergency landing, storm or no storm; or the many times I have been on flights that were delayed in landing because of heavy traffic and how this caused me to miss connecting flights; stories about some of the strange-looking aircraft I traveled on in Vietnam and in Central America; or some of the things that happened as we attempted to clear customs; or problems because of language barriers, etc. Incidentally, my trips have never allowed much time to see the sights along the way. Generally, I would work during the day, travel in the evening, or would be located at a God-forsaken place where there was nothing but work and wilderness.

I look forward to my next trip for the government; however, let it be known that such trips are not the same as, nor are they intended to be, vacations. I will always wonder, as I make future trips, what challenges I will face before I am once again home. I have gained a considerable education from these ventures and a new appreciation for the way things are back home.

The next time you have a chance to take a trip for the government, you should take it. Please, however, be prepared for almost anything to happen, as Murphy and his law seem to be nearby at all times. In fact, I think Murphy knows me well and is a constant traveling companion of mine. I have found that he is the only person who wants to travel with me – after people hear about my previous experiences. I don't mean to frighten or discourage anyone. After all, I am alive to tell my story. □

BULLETIN BOARD

EXCITING EXPERIENCES IN THE FIELD?

(C)   The Office of Archives and History (T54) is collecting historical information on field operations. They would like to hear from people who were involved in, or have information or files on, the following events:

If you can help, please call [   ] on 972-2355s. Or you may drop him a line at SAB-2, Door 22, T54.

WORKING ON CODES?

(C)   The Bookbreakers' Forum on Machine Aids will resume meetings this fall. Membership is open to individuals who work on codes as cryptolinguists, cryptanalysts, or programmers, or who manage or supervise such endeavors. To get on the mailing list send your name, organization, and building to: HQ, P16, [   ] Please do not phone.

P.L. 86-36

DO YOU HAVE THE MERCURY SOFTWARE?

(U)   The MERCURY software which [   ] advertized recently in Bulletin Board has gotten away from him. If you have it, or know who does, please give him a call at 963-1103 so that he can keep track of its whereabouts.

THE DISTRIBUTION OF CRYPTOLOG

At the request of Y16, Distribution, we have discontinued mailing labels. But to ensure that individuals continue to receive their own copies, we have instituted distribution lists.

A ROPE BY ANY OTHER NAME IS ... A TASSEL? (U)

B413
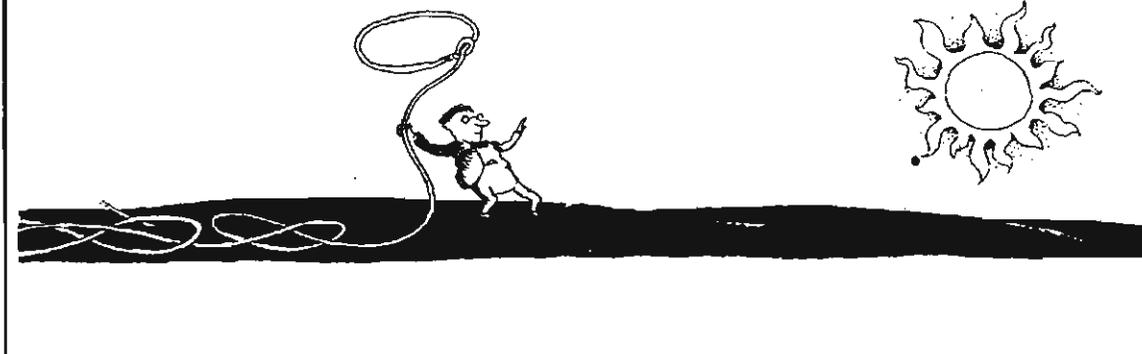
The true way goes over a rope which is not stretched at any great height but just above the ground. It seems more designed to make people stumble than to be walked upon.

Franz Kafka, *The Great Wall of China*

At the Asian Defense Technology Exposition in Beijing in November 1986, the People's Republic of China unveiled a new anti-submarine missile delivery system called the **Changying 1** (長纓), literally, "long tassel." This is an unusually vapid designator for a missile system, particularly as in the past the Chinese had used more virile names: *Sea Eagle*; *Red Flag*.

The origin of the name remained a mystery until the publication of the January 1987 issue of the People's Liberation Army Pictorial, featuring a four-page spread on the Beijing exhibition. The article did not mention the Changying 1. But the eyecatching headline provided a clue. It read:

Chang ying ke xi ri (長纓可系日)

which means,

The long tassel can tie up the sun.

It was obvious that the author was playing with words by using the name of the new missile in the headline.

I thought it might refer to a **chengyu**, which is a saying like "A stitch in time saves nine," something that literate (and pseudo-literate) Chinese often employ. An extensive search finally led to the discovery, in an obscure dictionary of chengyus, of two phrases with classic origins which were combined to create that headline.

One phrase, **chang ying zai shou** (長纓在手) literally means, "The tassel is in hand." Here *tassel* is used for *rope*. The classical meaning of the phrase is that with a rope in hand one can tie up one's enemies. Mao Zedong, the late chairman of the Chinese Communist Party, used the phrase when, impatient at waiting to conquer his enemies, he wrote: "Now the long tassel is in hand. When will it bind up the old dragon?"

The other phrase, **chang sheng xi ri** (長繩系日) literally means, "using a rope to tie up the sun." It connotes making an effort that cannot succeed, something like our phrase "to hold back the dawn."

Thus, the headline is ostensibly saluting Chinese weapons production, prominently featured at the Beijing exhibition, for doing the seemingly impossible. The indirect reference to the name of the new Changying missile is apparently an in-joke for the cognoscente, a quiet statement that Mao's successors have a new weapon with which to tie up their enemies. □

ODE TO STONEHOUSE

STONEHOUSE
    Tentative
        tenacious;
            Real . . .

GLASSHOUSE
    To some,
        Beware, do not throw stones;
    We will close you.

STONEHOUSE
    For those of us who know it,
                Real . . .
   We live it;
      We live.

STONEHOUSE
    On paper a Mission and Function;
      Stark words,
    Not even full of sound and fury;
      In bureaucratic jargon, certainly signifying nothing
    To those who do not know YOU.

STONEHOUSE
    To those who can see only shallow:
      A thorn,
        An O & M,
          A $, to be cut in trying times . . .
    Possible embarrassment;
      A THING, over there;
        A God-forsaken THING?
    Who cares? Or, is it who could care?

STONEHOUSE,
    To those of us who live it,
             Love it . . .

OURHOUSE

You there;
> do NOT throw stones at OURHOUSE!
We will not run.

In fact, even now you find we say:
> "Look at us, see what we do for you,
> Potential - see what we can do . . . "

You are not so blind;
> Perhaps you see a hint of what we say.

STONEHOUSE,
> Conscious,
>> Conscience,
>>> Observe,
>>>> Listen to OUR message.

Can you really close us?

> Measure the intangibles, mate;

Can you really replace us?

> Think hard, before it is too late.

Can you do without us?

> Know, before you seal our fate.

Can you still support us?

> Examine your returns to date.

Can YOU really face US?

> On this, do not procrastinate.

STONEHOUSE ...

POWERHOUSE

Dynamo pulsing strong through day and night;

    Curious mixture of stone, iron, and steel

With transistors, electrons, voltage, light;

    S E C R E T, Mission Impossible come real?

Dynamo with antennae at great height,

    Probing communications from afar;

Firm, poised steadfast and thriving from this site

    Security for Earth about its star.

Dynamo of people who take delight

    In computers, amplifiers, hardware;

Cabling to function with purposeful sight,

    And directing it with complex software.

Dynamo struggling through its daily plight

    With its machines made to produce for man,

To couple with his brain, avoid the blight

    Of resorting to our guns, if we can.

Dynamo striving with our free world's might;

    Ever hoping that IT will never cease

To support that which we believe is right –

    Liberty, justice, love – preserve some peace.
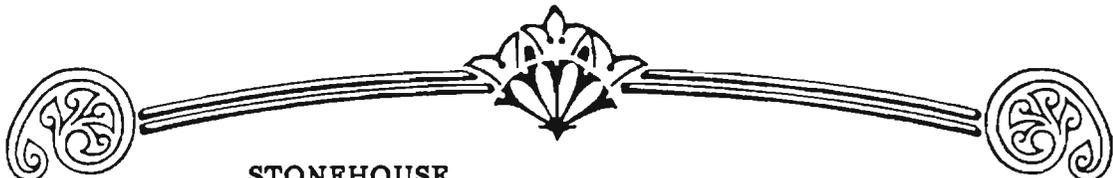
STONEHOUSE . . .

OUR HOUSE . . .

Security, our defined objective;

    Assigned mission for which OUR HOUSE does strive;

Technical and human strengths collective

    Unified to create a STONE alive.

Security, for memory:

    "A Mile High, A Mile Ahead;" trite, you say;

Perhaps. But for which we're appreciative

    To evoke emotions some far-off day.

Security: measures preventative

    With the proper tools, right time, correct place;

That's why it was not by chance creative

    [   ] was chosen STONEHOUSE base.

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

Security, no less diminutive

    For our great country in its ongoing strife,

If in honesty we are cognitive

    That we find here a satisfying life.

Security, of course, we're subjective

    In our judgment of this HOUSE's true worth;

However, there is still much substantive

    Beyond our feelings to warrant STONEHOUSE's berth.

Each person, from his perspective, will perceive

His own STONEHOUSE; many versions we will contrive;

We must avoid creating those that may deceive,

And with objective honesty we all must strive

To clearly portray the truths we deeply believe

When asking yea or nay to keep STONEHOUSE alive.

Key in this is whether or not we can achieve

Creation of a "STONEHOUSE" elsewhere that will thrive.

I know that there may come a time when I will grieve,

If when all is considered, STONEHOUSE you will rive;

There will be a part of me that will never leave

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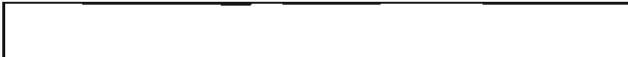
P.L. 86-36

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

[1st Issue, 1987] reminded me that I had written an Ode to STONEHOUSE when I was leaving it for the last time.

I dug back in my memorabilia file and found a copy. It evokes personal memories and emotions for me, of course.

This was written at the time when there was considerable controversy and anxiety over whether or not the STONEHOUSE facility should be closed. The Ode implicitly carries the messages of Dave's two tendencies, which he spells out at the end of his article.
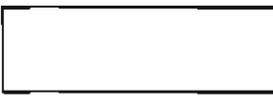
P.L. 86-36

CRYSCOM

A538/P13

P.L. 86-36

FOR OFFICIAL USE ONLY

The Cryptanalytic Software Committee (CRYSCOM) was established in May 1984 as a volunteer organization. CRYSCOM's major functions are: to provide a forum where representatives of the cryptanalytic supercomputer complexes can discuss issues of common interest; to collect and distribute critical information to the user organizations; to organize and conduct the annual Cryptanalytic Software Conference (CRYSCO); to carry out the recommendations made at CRYSCO; and to facilitate the development or maintenance of software for the supercomputing cryptanalytic community.

CRYSCOM consists of a Chairman, Vice Chairman, Executive Officer, representatives with voting privileges, non-voting members, and points of contact. The Chairman presides at meetings of CRYSCOM and the Executive Council, appoints standing and ad hoc subcommittees, and represents CRYSCOM where required. The Vice Chairman acts for the Chairman in the latter's absence.

The Executive Officer is the only individual working full time on CRYSCOM business. Responsibilities of the Executive Officer include: overseeing the execution of the CRYSCO/ CRYSCOM recommendations and reporting progress to CRYSCOM; recording the proceedings of the CRYSCOM meetings and distributing the minutes to the cryptanalytic community retaining documents that are generated through or on behalf of CRYSCO/CRYSCOM in the CRYSCOM Library; maintaining contact with all complexes; carrying out the wishes of

CRYSCOM and acting as a central point of contact for CRYSCOM matters.

The Executive Council determines CRYSCOM's policies and activities. The Council includes CRYSCOM representatives from each of the supercomputer complexes, the CRYSCOM Executive Officer, and one representative each from B6, T335, and T442.

CRYSCOM representatives who have voting rights are chosen by their complex manager. As representatives, they pass information to and obtain information from the user groups they represent. Since CRYSCOM has no power or authority, it must rely on the consensus of its members to implement new ideas and to solve problems.

Membership is open to interested persons in organizations which perform and support cryptanalysis in the supercomputer complexes at NSA. As a member, an individual has no voting rights but may voice concerns at the monthly CRYSCOM meeting.

CRYSCOM has points of contact in each of the supercomputer complexes. They are the main contacts for cross-complex transactions. They assist in coordinating software and information exchange between supercomputer complexes, and also assist the CRYSCOM representatives in communicating information to, and receiving feedback from, users.

P.L. 86-36

The monthly CRYSCOM minutes are sent to 65 individuals. The minutes as well as other items of interest are available in CANEWS, an on-line user news file residing on all the systems. □

LETTERS

To the Editor:

I was glad to see the plea in the December 1986 issue of CRYPTOLOG for a readable computer handbook. Certainly it was time that there was public recognition of how poorly the job of introducing computers into our workspaces has been done. If the people who make the decision on the hardware, software, and training for the ASTWs and other desktop computers know how to automate a workplace properly, they have done a good job of keeping the fact a secret.

I know enough about computers to discuss them, but no so much that I cannot discuss them in English any more. I have a microcomputer at home, and I have as friends a software engineer and a computer secrity officer, and my father is a computer systems consultant. From them and from my own reading on the subject, it is clear that most of the usual steps in automating a workplace have been ignored here.

There are three basic steps to putting computer systems into the workplace. First, an expert knowledgeable in hardware, software, and other components of computer systems comes to the actual work area to be automated. This person will examine how that office does what it does and will suggest a system to meet each area's needs. Next, budget and compatibility questions are addressed: what can be afforded and will it work with any equipment already in place? Last, the system is installed and the users given training on it. A fourth "step" is the programming and service support so that the system continues to run and to evolve to new needs after installation. This step, at least, is being done well and need not be discussed further.

Our office got the same computers with the same software for everyone: no tailoring to our particular needs. The computers have actually made more work for us and slowed down the process of getting reports out. As for budgeting, it appears that we could have paid some 30% less than we did. Our PC/XTs communicate well with the mainframe systems when used as terminals, but have limitations in their ability to work with the PC/ATs we were given just recently. And, as the plea in CRYPTOLOG for a handbook shows, we are still waiting to find out how to use our computers.

Of course, the standard answer to training requests is "Read the Manual." But the manual is barely comprehensible, full of technical terms unintelligible to most people. And much if what is in the books is for the programmers and systems management people, not for the average users with PCs on their desks. Which commands are for which people, and how do you apply the commands that are for you?

The User's Handbook for the PC/XT is a dictionary of commands. It is like buying a toolbox and having a manual which tells you, in technical detail, how to operate each tool. But what we, the average users need, is the computer equivalent of a home improvement "How To" book. Most people do not even know the questions to ask on how to apply their computer to their job. A typical exchange:

"What can I do with my computer?"
"What do you want to do with it?"
"Gee, I don't know. What can it do?"
"Oh, it can do all sorts of things, but what do you want to do with it?"
"Well, what can it do?"

There are millions of dollars with of unused and underutilized computer capacity sitting on desks all over the Agency because the users really have no idea how to use them fully. If the Agency is serious about combatting waste, it could save a lot right here.

B41

Maybe the authors of future works on using PCs will refer to pp 25-26 for guidance on writing directions.   Ed.

To the Editor:

In response to your editorial in the December 1986 CRYPTOLOG ("Julia Child, Where Are You?") I would like to point out that there have been attempts to simplify the documentation for personal computers. The problem is often not that a usable handbook doesn't exist, but that the existence of that handbook is known only to a small group.

In particular, when G74 first began receiving IBM PC-XT prototypes for the ASTW, I wrote a manual for analysts using these machine with PC/IX. (This manual is usable with the XT-based ASTW as well, but some keys are in different places on the keyboard.) While it is far from perfect, my manual is an improvement over the IBM manuals both in readability and in usefulness, as it has an index. This manual is widely distributed in G74 but, while I provided copies to G3, T4, and ASPIC, its existence seems to be one of the better-kept secrets around here.

I am sending you a copy as a separate e-mail message. If you find it useful, please feel free to pass it on to anyone who could benefit from it. If you feel it needs improvement, please feel equally free to pass it on to let me know what changes you think are necessary.

☐ *G743*

A sample page of Barry's manual appears on Page 23.   Ed.

To the Editor:

I read your editorial in the December 1986 issue of CRYPTOLOG with great interest because you were talking about the need for materials to help novice PC users. Help is available in the Agency Standard Products Information Center (ASPIC, formerly the PCIC)! Enclosed are some samples. Unfortunately, because of legal constraints, we cannot include material such as these in the IBM boxes when they are delivered, but they are readily available in our OPS-1 and FANX-III locations.

In addition to these written aids, we have analysts ready to handle problems on the phone. We have tutorial packages that can be borrowed for up to two weeks at a time. Nearly all of our applications packages include excellent tutorials to help people get started.

☐ *A/Chief, T535/ASPIC*

A sample page of the ASPIC manual appears on Page 24.   Ed.

Have you missed these articles?

§ "Has It Ever Been Translated Before? Tracking down technical translations." by ☐ Jul-Aug 1978

§ "Exercise Support." by ☐ December 1981.

§ "Rules for the Camel Corps." by ☐ March 1982.

§ "What Promotion Boards Want." by ☐ August 1982.

§ "Arms Control in the Wake of KAL 007." by ☐ April 1984.

§ ☐ by ☐ Jan-Feb 86

§ ☐ by ☐ Mar-Apr 86.

§

To obtain a copy, send your name, organization, and building to: Editor, CRYPTOLOG, P1, HQS. Phone requests will not be honored.

§

Yes, we recycle!

We're always happy to receive back copies of CRYPTOLOG, especially of these recent issues: Oct-Nov 86, Dec 86, 1st Issue 87, 2nd Issue 87. We'll also accept copies of CRYPTOLOG's predecessors,: *KEYWORD, Dragon Seed, COMMAND, The Quarterly Review of Linguists.*

Sample Page:

USER'S MANUAL FOR PC/X ON THE UIS PROTOTYPE. *by* [   ] *G743*

PC/IX Manual   1 January 1985

built-in hardware tests will be performed, during which time
a series of memory check reports (e.g., "320 KB OK") will
appear on the screen. When the tests are complete, the sys-
tem will beep once, try to read from the floppy drive, try
again, and finally begin loading from the hard disk. During
the loading process, the statement "booting /uni> from par-
tition 1" will be displayed. After a short time, there will
be another beep, the amount of available memory will be
displayed at the bottom of the screen, and the following
notices will begin to appear:

        Normal startup in progress.
        File system integrity assumed.
        Enter Date [[MM]DD]HHmm[YY]:

Type in the portions of the date and time which have changed
since the last time the system was booted. (I.e., if this
is the first time on 19 Oct 84 that the system has been
turned on, but it was used on 18 Oct, enter the day and
time.) The format to use is two digits each for the month,
day of month, hour, minutes, and year. The hour and minutes
must be entered, the other three fields may be entered, but
are only required if there has been a change since the last
startup. Some additional system notices will be displayed,
then the screen will clear and the login prompt will appear.

B.   Login

        At the login prompt ("login:"), type the name by which
you are known to the system (usually your initials). The
computer will respond "Password: ". Enter your current
password. If your password has expired (M), you will be
asked to supply a new one. After entering the new password
a second time, you will be presented with a new login
screen. Log in once more, using the new password. (Note
that this is different from the PDP-11/Delta Data system,
which allows you to log in using the old password, but asks
you to use passwd to change it. PC/IX automatically runs a
modified passwd when you try to log in and then logs you out
again.) Once you are logged in, the system prompt (a dollar
sign, rather than the percent sign we see on the Delta
Datas) will appear and you are ready to begin work.

C.   System Commands

        When you consider that Section 1 of the IBM PC/IX
User's Manual is 1.7 centimeters (about 2/3 inch) thick, you
begin to get the idea that there are probably a lot of sys-
tem commands which you will rarely, if ever, use. This
guide, however, will try to present the most generally use-
ful system commands as clearly as possible. In the entries

                          -7-
                      UNCLASSIFIED

Sample Page:

TIP SHEET: INTRODUCTION TO THE ASTW: *Issued by ASPIC (formerly, PCIC)*

INTRODUCTION TO THE ASTW   Page 3

    The Login: prompt will then be displayed.

4. Log in using your user ID and password (if one was assigned
    by the system administrator; if not, press the Return key).

    System: Login:
    User: (enter your login identifier)

    System: Password:
    User: (enter your password)

    System: $

5. Set the battery-back-up system clock.

    Key the numeric month (mm), day (dd), hours (hh), minutes
    (MM), and year (yy) after the clock command as follows:

    System: $
    User: /priv/clock mmddhhMMyy

6. Activate the "-" mode of the -/Lang key. (Note 1.)

    Press the Ctrl and -/Lang keys simultaneously. (The "-" mode
    is required by the INed program to implement the Cancel
    command.)

7. Do the INed tutorial.

    Read and follow the INed beginner's tutorial as defined in the
    PC/IX Text Processing Guide section that begins at the
    Getting Started tab. This tutorial provides valuable
    instruction on the PC/IX page editor and introduces file
    structure concepts as well as many of the more popular PC/IX
    commands. We strongly urge that you complete this tutorial.

8. Establish your password.

    Invoke the Password command and define a six-or-more character
   password that will be required at each future logon:

    System: $
    User: passwd

    System: New password:
    User: (key your desired password)

    System: Re-enter new password:
    User: (key your desired password again)

    System: $

* The PC Information Center * Room 1S042 * 963-4670 * 12/07/84 *
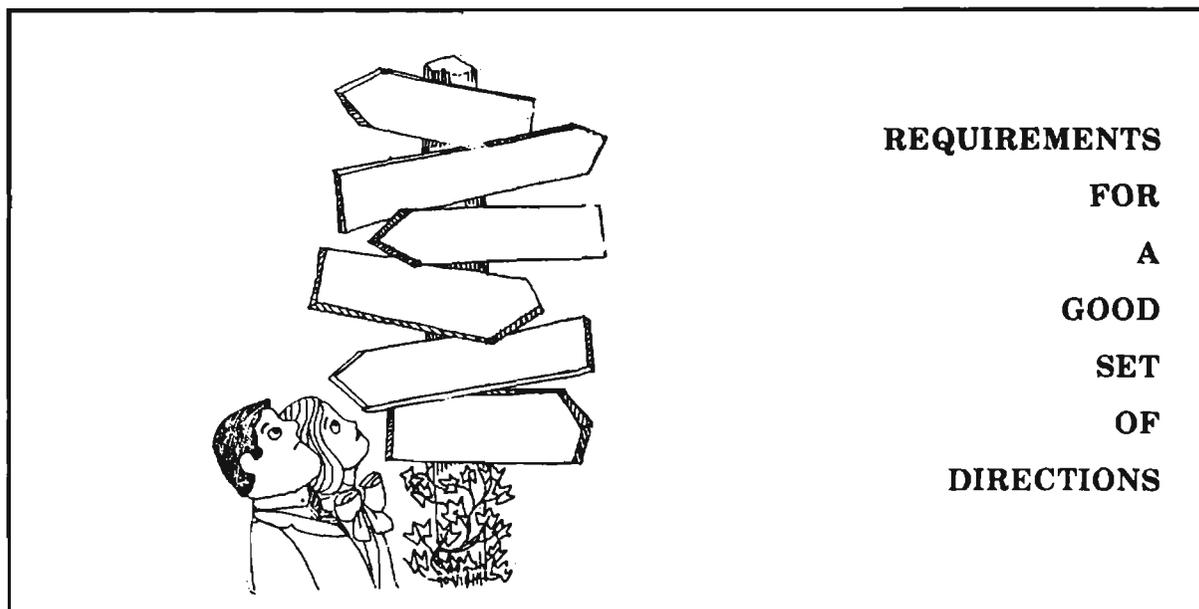
REQUIREMENTS FOR A GOOD SET OF DIRECTIONS

extract from: *Writing Scientific Papers and Reports*. by W. Paul Jones, revised by Michael L. Keene.

W. C. Brown Company, Publishers. Dubuque, Iowa. 8th Edition, 2nd Printing, 1982 [PE 1475 .J72 1981]

1. Completeness

Keep your readers constantly in mind. Are they laymen, executives, experts, or technicians? Whatever the case, write for those within the group who know least about your subject. They will need every aid you can give them. Experts can ignore the directions if they don't need them.

2. Explanation of Technical Terms

Lest any reader may not understand them, define and explain your technical terms. Experts can skip the explanations, but non-experts may be frustrated without them. Most people don't have technical dictionaries to which they can refer.

3. Proper Emphasis

Number each direction and devote a whole paragraph to it, even if it is only a single sentence. Readers can then check them off, thinking, "All right, I've taken that step. Now what's next?" The next numbered paragraph will tell. If you include two or more directions in a single paragraph or under a single number, readers are likely to overlook one of them. Allow plenty of space for each direction.

4. Use of Visual Aids

Include any diagrams, pictures, graphs, etc. that will help readers to follow a direction.

5. Reference to Visual Aids

Put visual aids where the reader can most easily refer to them. If such an aid can be on the same page and near the direction it concerns, it will be most conveniently placed. If it is on a different page, readers may not refer to it when they should, and consequently may misunderstand a direction. Your own experience will tell you how irritating it is when a textbook prints a diagram, picture, table, graph, etc., on a different page from the explanation of it. If it is impossible to place it on the same page, put it on the next page.

6. Explanation of Visual Aids

Don't fail to allude to, if necessary explain, any visual aid. Usually it is not enough merely to refer to it, as in writing "See Figure 1." Add any explanation that will help reders to follow your directions. Too often the writer assumes that the meaning of a visual aid is self-evident and leaves many readers to puzzle out its meaning for themselves.

7. Justification for a Direction

Be sure to give the reason for any direction, especially if your readers might think, "Why do that?" Otherwise, they might follow a different procedure which seems at the moment preferable.

8. Explanation of General Principles

Explain any general principles that readers ought to understand if they are to follow your directions easily. If the principles underlie the whole procedure, explain them in the introduction. If they refer to only one direction, put the explanation after the direction.

9. Suggestions for Avoiding mistakes.

Warn readers when there is a possibility of making a mistake. Novices especially may need warning to prevent wasting time or ruining expensive equipment. Mistakes due to lack of experience or skill may not be avoidable, but those due to ignorance or carelessness are inexcusable. If, for example, your instruction emphasizes the importance of gluing a wood joint instead of nailing it, you may prevent someone from making something that breaks under stress. Such warnings should be placed at the beginning of the set of directions. Do not assume your reader will read all the directions before starting the process. Your own experience tells you that the natural tendency is to follow instructions step-by-step without first reading all of them.

10. Avoidance of Telegraphic Style

Don't leave out all words like *the* and *a*, or the subject of verbs, words necessary for full grammatical expression. Telegraphic style may be justified if space is limited, as on bottles and other small containers. But in the average set of directions you will save less then 5 percent of your space in using it. Furthermore, telegraphic style is likely to obscure the thought. Instead of "Put curd into bowl, add water," it is better to write, "Put the dried curds into a small mixing bowl and add 4 tablespoons of cold water."

11. Consistency in Point of View

Use the second person imperative whenever you are writing a direction. For example, you should say,

Pour two cups of skim milk into the saucepan.

not

You should pour two cups of skim milk into the sacucepan.

or

Two cups of skim milk are then poured into the saucepan.

The last two are not imperative constructions.

But if you are stating a general principle or giving some useful supplemenary explanation, use the third person. For example, after a direction "Add 6 tablespoons of vinegar to the milk," in the same paragraph could follow the explanation, "The vinegar will sour the milk and precipitate the casein out of the mixture as curds."

12. Use of Clear Transitions.

Make all of your transitions from section to section and from direction to direction as clear as possible. Proper used of headings, numbers, and paragraphs indentations will usually be sufficient. Don't insert unnecessary transitional words and phrases. If direction 3 is "Add one teaspoon of bicarbonate of soda," direction 4 should begin, not with "then" or "now" or "after you have done this," but simply with a new paragraph, the number 4, and the verb in the imperative: "4. Continue the blending, etc." Sequence in time ordinarily governs the arrangement of directions. Only if two or more things are to be done at the same time would a transitional phrase like "at the same time" or some explanation be needed.

PLAN FOR A SET OF DIRECTIONS

The plan for a set of directions is essentially the same as for a description of a process. In developing the plan, however, you need to pay special attention to the division points, both major and minor. Remember that your readers are, presumably, going to perform the process with your directions as the only guide. If they misunderstand a point in the description of a mechanism, perhaps the loss is not serious, but if they misunderstand a direction, they may lose a lot -- including their temper. □

BOOK REVIEWS

Her Majesty's Secret Service: The Making of the British Intelligence Community. By Christopher Andrew. Elisabeth Sifton Books, Viking, New York, 1986; pp. xviii, 619.

Reviewed by: Vera Filby, E4

The name Christopher Andrew is becoming familiar to readers of the British press. Dr. Andrew, Fellow and Senior Tutor in History at Corpus Christi College, Cambridge, is called upon with increasing frequency to comment on books and events of intelligence interest, like the Peter Wright affair in Australia, which was in the news at the time of this writing.

Dr. Andrew brings a message as well as a solid and scholarly account of British intelligence history in the 600 well-packed pages of his book. His message is that histories of 20th century British politics, foreign affairs, and military matters cannot be accurate or complete if intelligence is not taken into account, but British government, law, and tradition have unyieldingly blocked release of peacetime intelligence. Dr. Andrew maintains with some passion that the government should recognize that this is unreasonable and should release to the public archives all records that can do no harm to national security. (Those of us in the business can sympathize, but we understand that security decisions may not be as unreasonable as they seem to researchers on the outside looking in.)

After a glance back at Queen Elizabeth I's secret service, Dr. Andrew briefly traces the development of the British intelligence services up through the Boer War and into the 20th century. As early as 1703 a "Decyphering Branch" was set up by the Secret Service Fund. This largely private enterprise, as well as other intelligence and covert activities financed by the fund, were carried out by freelance amateurs and gentlemen adventurers. Indeed a trace of the amateur tradition survived even into recent times. The Decyphering Branch was disbanded in 1844, a time which, as Dr. Andrew points out, was exactly wrong, since the electric telegraph was just coming into use.

The progenitors of today's intelligence and counterintelligence services were created by strong-minded civilian officials and military men who saw unmet needs for intelligence and took action to do something about meeting them, usually battling the "venerable inertia" of the established order. It was not until 1886 that the Naval Intelligence Department was created, and that was against the will of the Board of Admiralty.

The civilian intelligence organizations were also slow in getting started. Such resources as the counterintelligence agencies did muster were largely occupied trying to cope with Fenian violence. In 1884, after a bomb was set off in a public lavatory in Great Scotland Yard and security measures were being implemented, it was found that the entire sanitary system of the Houses of Parliament was being overhauled by Irish workmen.

When the Boer War started in 1899 the War Department's Intelligence Division had a total of 18 men with 2 officers and a clerk responsible for all British colonies and protectorates and the Boer Republics. When intelligence officers were sent to the field, their reports were disbelieved or ignored, but after the shift to guerrilla warfare a large and well-organized Field Intelligence Department was formed. As happened after other wars before and since, the intelligence structure did not survive the victory.

Boer guerilla successes shook British faith in the invulnerability of the empire. With the regular army overseas, fear of invasion by France washed over the country. Later Germany became the country to fear, and the hunting of spies, real and imaginary, occupied the counter-intelligence forces. During the same period the organization which was the ancestor of the Secret Intelligence Service (SIS) was founded. The first chief, Commander Mansfield Smith-Cumming, or Cumming for short, was the source of the designation "C," still used for the chief of SIS. He was another of the colorful characters that have populated British intelligence history. The fact that logbooks he kept are still considered too sensitive to release provides Dr. Andrew another opportunity, which

he is glad to take, to point to the absurdity (as he sees it) of withholding information so old that it could not conceivably be injurious to national security.

The peacetime exploits of the counterintelligence agents may have been often ineffectual, but peacetime cryptologic efforts were non-existent. So upright was the Foreign Office in this regard that the Cambon brothers, French ambassadors in London and Berlin, used the British diplomatic bag, considering it more trustworthy than the French post or diplomatic couriers.

The 1914-18 War changed all that. The inadequacies of the old ways of gathering information at sea got the attention of the First Lord of the Admiralty, Winston Churchill. From the beginning, even as far back as the Boer War, Churchill understood and valued intelligence.

What was to become the famous Room 40, named for its location in the Admiralty Old Building, began with the appointment of the Director of Naval Education, Sir Alfred Ewing, to do something about coded messages thought to be of enemy origin. The effort began with a group of six mathematicians and linguists who according to one of them were "singularly ignorant of cryptography." They had to work in shifts because the space provided was too small. From that beginning, Room 40 grew into a formidable company equalled in accomplishment, brilliance, and general oddity only by its descendant, the phenomenal creation also named for its location, Bletchley Park. Room 40 knew failures too, but often they were failures not of the cryptanalysts but of the intelligence evaluators and disseminators. Much of the accomplishment of cryptanalysts on both sides was due to the lack of any sense of security on the part of their opponents. U-boat commanders, for example, helped Room 40 considerably by their "extreme garrulity." Nevertheless, German security did take effective measures from time to time, and during one of the periods of unreadability, a group of Room 40 people got together in a separate room to experiment and find out what they could do with the externals alone, and they invented traffic analysis, though they had no name for it then.

Just as there was no effectively organized foreign or naval intelligence at the beginning of the war, neither was there an organization for field intelligence until a commandant for an Intelligence Corps was appointed in 1914. The author tells the history of the Corps' operations on the Western Front until Armistice Day, when the last weekly Order of Battle showed the location of 186 enemy divisions. Only two proved to be wrong.

In 1919 a peacetime cryptanalytic group, which was eventually named the Government Code and Cipher School (GC&CS), was formed with veterans of Room 40 and the War Office MI1b. Wasting no time, they were soon reading French, American, Japanese, and Soviet traffic. Evidence of Soviet agitation and subversion, supporting the revolutionaries in labor unions and among disaffected ex-servicemen, was so overwhelming that in 1920 outraged government officials were determined to expose it, and did. Even Churchill approved. In 1923 the government issued an ultimatum to the Soviets charging subversion and other hostile acts and quoted verbatim extracts of decrypted message texts. In 1924 a letter from Zinoviev, a Comintern official, was leaked for political reasons, and two days later a debate developed into "an orgy of governmental indiscretion." The eventual Soviet response was one-time pad, and GC&CS was out of the Soviet dip business.

With the onset of the depression, Britain's military power went into a steep decline and along with it military intelligence. Counter-intelligence MI5 also suffered shortages of resources despite continuing Communist hos-tility. GC&CS, though lean and hungry, still exploited Japanese, Italian, Comintern, and other traffic (while some of the source countries did pretty well with British traffic). A great triumph occurred in 1933, when a team under Colonel Tiltman (our own "Brig," whom many of us remember with admiration and affection) broke into Comintern traffic from Moscow to a terminal which was DF'ed to a house in a Lon-don suburb. This was GC&CS' first use of DF. The law did not permit a search of the house, but MI5 finally got hold of one of its contents, a pamphlet "intended to be issued to the Fleet containing a gross incitement to mutiny."

After many years of preoccupation with inimical forces from the left, dangers from the radical right appeared with the fascist movement in Britain. But this menace never matured, and by the time the wave had passed

in the mid-1930's Germany had replaced Soviet Russia as the main worry for foreign intelligence. By then the Passport Control Office, which for years had been the cover for foreign intelligence operations, was being overwhelmed with applications from Central European Jews to go to Palestine. GC&CS successes during those years were often defeated by ill-coordinated intelligence evaluation and dissemination and by atrocious personnel and physical security in British embassies.

Intelligence events in the early days of the war included revelations by a defector of traitors in communications and the gift of the priceless but officially unappreciated Oslo Report, obviously written by a scientist, which contained information on new German torpedoes, radars, and other developments including early rocket work and the experimental center at Peenemunde. (*The Griffin*, published in 1986, is a biography of Paul Rosbaud, science editor for a German firm, who the author, Arnold Kramish, believes was the source of the Oslo Report.)

The thrust of Dr. Andrew's relatively brief treatment of the years from May 1940 when Churchill took office to 1943 is expressed in the chapter title, "Winston Churchill and the Making of the British Intelligence Community." Churchill had always believed in, appreciated, and championed secret intelligence. His faith in what was not yet called COMINT was rewarded when GC&CS, by then renamed Government Communications Headquarters (GCHQ), broke into an Enigma system. This was a payoff for foresighted cooperation with the Poles and the French.

GCHQ was foresighted also in the quiet recruiting beginning two years before the war of some of the best classics, language, and mathematics brains in Cambridge. The service intelligence departments were slower getting started, but they gathered in naval veterans of Room 40 and high quality men from the financial world. One of them was the stockbroker Ian Fleming. MI5 was even less prepared. Those it began belatedly scooping up included some of the most colorful intelligence characters as well as six future judges, future university professors, and Anthony Blunt. The Secret Intelligence Service was not in the same class, though some of the recruits became famous personages, among them Malcolm Muggeridge, Graham Greene, and Hugh Trevor-Roper. One other recruit was the only one to earn a decoration for his wartime work. His name was Kim Philby.

Exiled foreign intelligence services added to the assets available, and SIS maintained liaison with the Czechs and Poles and kept communications and funding control over the Norwegians, Dutch, and French. The operations, exploits, dirty tricks, misadventures, and coups of SIS and MI5 have became famous through the many histories, biographies, autobiographies, memoirs, spy stories, and films based on them in the years since.

Dr. Andrew credits SIS with two pioneering developments before the war. One included new methods of photoreconnaissance and a commercial front organization to carry them out. By the time the war started and the enterprise had been turned over to the Air Ministry, large parts of Germany and the Mediterranean had been photographed. The other innovation was the creation in 1938 of Section D (for Destruction) to specialize in means other than the operation of military force, translated as dirty tricks. This, as might have been expected, attracted some extraordinary people, one of whom, Guy Burgess, would eventually be exposed as a traitor.

Intelligence produced by all these outfits remained ill-coordinated until the Joint Intelligence Committee was bolstered by a Joint Intelligence Staff. In this improved coordination as in other aspects of intelligence, Churchill was directly involved. His interest and influence were strong, creative, and personal. Under his inspirational leadership, the author concludes, "the fragmented intelligence services acquired that degree of coordination which turned them into an intelligence community."

In the epilogue, "War and Peace," Dr. Andrew agrees with the now generally accepted opinion that signals intelligence made possible the victories in North Africa and the success of the Normandy landings. He summarizes in a few pages the main events in British intelligence since the war – the intensive and continuing collaboration between Britain and the United States in SIGINT; the revolution in air reconnaissance, first by the U-2, later by satellites; spies, more spies, moles, and defectors; and the still undiminished strength of the traditional taboos against discussion of the

intelligence community and release of information on peacetime intelligence activities.

This is a hefty work intended for serious readers, but Dr. Andrew's style makes it a pleasure as well as an education to read. Touches of wit and a dry humor come through especially in his accounts of spy-counterspy goings on. Some of these stories are too far out to be anything but true. ☐
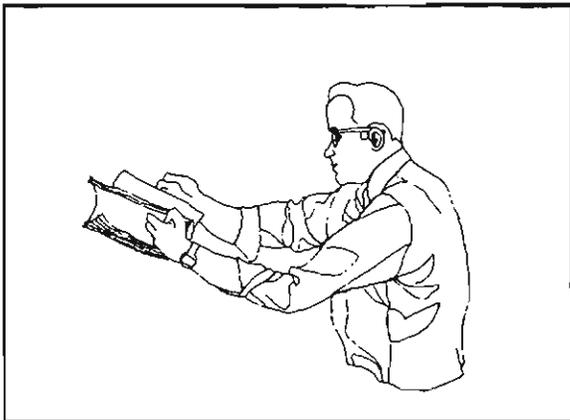
Teleconferencing [a set of 37 papers] edited by R. Rao and R. Srinivasan, Van Nostrand, 1985

Reviewed by: [   ] *P13*

This book is well edited and filled with information, and should be within reach of anyone concerned with high-bit-rate digital traffic. The papers aptly reveal the progress in video coding.

Video teleconferencing is gaining in popularity as a means of conducting business meetings. Two key factors in the spread of video conferencing is the digitization of the video signals and the use of compression coders to reduce the bit rates needed.

The first one-way videotelephone transmission took place in 1927 between New York and Washington D.C., and a two-way system, between Bell Labs and AT&T New York headquarters, took place in 1930. In 1971 the Picturephone service was introduced by AT&T. 3-bit DPCM coding was used to reduce the bit rate to 6.3 Mbps, carried on a T-2 digital carrier, which was technically advanced at that time, but the service did not have many customers. Satellite transmission changed that, and now a wide variety of teleconferencing

services is available in European countries under the umbrella of the EUTELSAT, a consortium of 20 countries in the European Telecommunications Satellite Organization. At present, the substitution of videoconferencing for business travel amounts to only 0.003%, but this is expected to increase to 6% by the 1990's, (more than a 1000 fold increase), according to a NASA study included in the book.

The fundamental problem of providing video teleconferencing is the signal bandwidth and the cost, which are linked. In the US, analog transmission of video using "soft" video scrambling has been done, but the international trend seems to be digital compression. A seven-nation European COST 211 project resulted in a transmission format and a codec to operate at the CCITT 2 Mbps rate. It will code both European 625-line and US 525-line video frames. Encryption will be available using the DES algorithm, according to the author of Paper #23, and a public key exchange was planned.

The video coding techniques can be classified into two categories, predictive coding and transform coding. The 8-bit PCM coding of a video frame requires 90 Mbps, but different coding techniques described in the book show how this can be reduced to much lower rates.

"Full motion" codecs can operate in the 6.3-to-.5 Mbps range, and a number are already on the market. The dedicated T-1 1.5 Mbps carriers cost $30,000 per month, so there is a search for lower bit rate codecs. A British GEC codec at 1.5 or 2 Mbps is widely used in Europe. NEC also has produced an excellent codec with motion compensation --- to give smooth picture continuity when rapid subject movement occurs.

Part IV of the book is concerned with codecs that work in the range from 320 Kbps down to 4.8 Kbps. Many users accept the lower quality of 56 Kbps codecs to avoid the high costs of the T-1 carriers.

As ISDN and IDN services provide 64 Kbps channels to subscribers' premises, the 56 Kbps codecs will become easier to use. There is a lot of product competition at each of the tariffed bit rates (6.3, 1.5 Mbps, 56, 9.6, 4.8 kbps) and these coded communications are certain to form an increasing part of future digital traffic. ☐

From the past
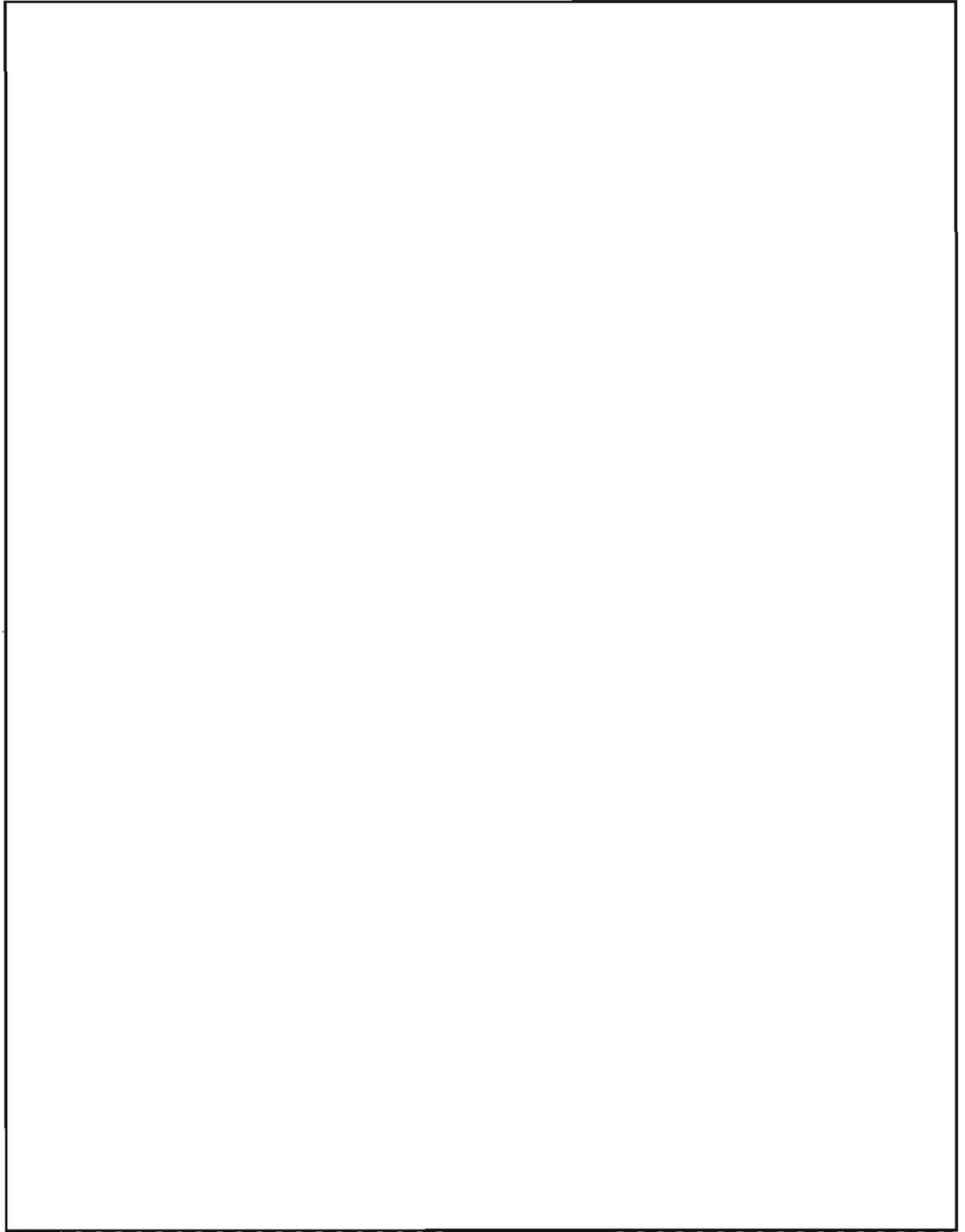
Contributed by: [   ] A112

P.L. 86-36

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

NSA-CROSTIC #65

P12

> The quotation on the next page was taken from a plaque in the building. The first letters of the WORDS spell out the author's name and the title on the plaque.

DEFINITIONS

A. Navy cryptanalyst, Battle of Midway fame

B. Unrestrainedly frank

C. Boreal phenomenon (2 wds)

D. Stage orphan

E. Photons, not meager mantas (2 wds)

F. Haggard; depicted

G. Perhaps the shortest everyday word with 4 Rs.

H. Issues

I. Nevertheless

J. Askew

K. Versatile aircraft

L. State named by its British discoverer after his homeland (3 wds)

M. Maine (2 wds)

N. Tout le monde

O. A 32nd note

P. Zoological specialty

Q. Fire

R. Of hearing

S. Voluble

T. Crush

U. Crushing

V. Holmes's chambered mollusk

WORDS

A. 23 94 88 37 66 206 4 17 45

B. 211 3 6 10 15 99 109 121 129

C. 194 115 91 27 40 8 207 173 123 71 55 60 80 162

D. 68 90 100 126 137

E. 127 98 146 70 141 28 42 142 113

F. 79 116 133 179 210

G. 168 48 164 13 33 65 82 86 101 122 143 147

H. 148 185 160 138 50 19 72 125

I. 12 54 124 67 29 201

J. 73 77 131 181 151 104 57 62 56 32

K. 108 84 22 7 186 183 180 176 170

L. 9 14 36 43 63 96 114 139 172 174 177 184 205

M. 192 208 212 102 128 135 152 157

N. 202 166 161 145 132 47 34 26 200

O. 103 191 197 58 69 92 107 112 118 144 149 154 167 204

P. 31 39 41 59 81 117 105 95 75 49 1

Q. 156 171 199 5 195 203 190 136 83 74 53 24 35

R. 21 119 30 38 97 2 64 196

S. 18 198 178 169 140 130 120 93 85

T. 163 51 20 16 153 188 11 175 87 158 76

U. 193 187 110 159 134 111 165 182 209 44 52 61

V. 78 89 106 150 155 189 25 46

HOW TO SOLVE A DOUBLE-CROSTIC

Using the Definitions, fill in whatever Words you can. Then copy each letter from the Words into the corresponding square of the grid. Scan text in in the grid from time to time; from the recovered fragments you may be able to complete the word in context. Copy the new entries in the grid into the Definitions, where the fragments might suggest the complete Word, and so on, working back and forth. Also, scan down the first positions of the Words as you recover them, for additional clues.

1P	2R	3B	▨	4A	5Q	▨	6B	7K	8C	▨	9L	10B	11T	▨	12I
13G	14L	▨	15B	16T	17A	18S	▨	19H	20T	▨	21R	▨	22K	23A	24Q
25V	26N	▨	27C	28E	29I	30R	31P	32I	33G	34N	35Q	▨	36L	37A	38R
39P	40C	▨	41P	42E	43L	▨	44U	45A	46V	▨	47N	48G	49P	50K	51T
52U	53Q	45I	55C	56J	▨	57J	58O	59P	60C	▨	61U	62J	63L	64R	65G
66A	▨	67I	68O	69O	70E	71C	72H	73J	74Q	75P	76T	▨	77J	78V	79F
▨	80C	81P	82G	▨	83Q	84K	85S	86G	87T	88A	89V	90O	▨	91C	92O
93S	94A	95P	96L	97R	98E	99B	100D	▨	101G	102M	103O	▨	104J	105P	106V
▨	107O	108K	109B	110U	▨	111U	112Q	113E	114L	115C	116F	117P	▨	118O	119R
120S	121B	122G	123C	124I	▨	125H	126O	127E	128M	129B	130S	131J	132N	▨	133F
134U	135M	136Q	137D	▨	138H	139L	140S	141E	▨	142E	143G	144O	145N	146E	
147G	148H	149O	150V	151J	152M	153T	▨	154O	155V	156Q	157M	158T	159U	160H	161N
162C	▨	163T	164G	▨	165U	166N	167O	168G	▨	169S	170K	171Q	172L	173C	▨
174L	175T	▨	176K	177L	178S	▨	179F	180K	181J	182U	▨	183K	184L	▨	185H
186K	187U	188T	189V	190O	191O	192M	▨	193U	194C	195Q	196R	▨	197O	198S	199Q
200N	▨	201I	202N	203Q	204O	205L	▨	206A	207C	208M	209U	▨	210F	211B	212M

THE ONE AND ONLY WINNER!

_____ R822, is the only person to report success in finding the PLUS in NSA-Crostic No. 63, December 1986. He is also the author of NSA-Crostic No. 64, 2nd Issue 1987, the solution to which is given on the right.


Solution to NSA-Crostic No. 64

[William F.] Friedman, Lecture V, *Six Lectures on Cryptology*, National Cryptologic School, 1965 p. 116.

No code, [no matter how carefully constructed,] will be safe without trained, intelligent personnel. A poorly constructed code may be [in reality more] safe(r) when used by an expert than a [very] well-constructed one when used by a careless operator, or one ignorant of the dangers of improperly encoded messages.

Like to try your hand at composing an NSA-Crostic?
For instructions address your inquiries to HQS, P1, Puzzle Editor, CRYPTOLOG.

TOP SECRET