~~TOP SECRET~~

JUN 1974?

National Security Agency

Fort George G. Meade, Maryland

FINAL EDITION

DRAGON SEEDS

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

This is *Dragon Seeds*.

There is fantasy, irony, and the bite of reality in the name. It speaks of the East. And, like the East, it suggests much, says little.

Dragon Seeds is both Mother China and her neighbors. *Dragon Seeds* is monumental and minuscule. It is the past and future. It begs for elaboration but gives none. In it are echoed softly slurred Mandarin, brittle Vietnamese, determined Korean. In it is the spectre looming over the Thai, Lao, and Khmer. It is frightening and friendly. It is uncertain.

Above all, *Dragon Seeds* is promise. It is fertile with ideas unbounded, to be cultivated with creativity and imagination. It is challenge. It is alive. It will be more than it is.

Dragon Seeds is yours. May it grow with you.

The Editors

PL 86-36/50 USC 3605

DRAGON SEEDS

JOSEPH R. BURGESS, CHIEF B4

Publisher

Managing Editor
Minnie M. Kenny

Feature Editor
Robert F. Kreinheder

Special Interest Editor
Ray F. Lynch

Rewrite Editor
Jane E. Dunn

Education Editor
Marian I. Reed

Composition
Louella M. Ertter

Press Corps

B1	Carolyn Brown	B3	Edmund J. Guest
B2	Jack Spencer	B3	William Eley
B2	Jean Gilligan	B4	George S. Patterson
B2	Louis Ambrosia	B4	James W. Schmidt
B3	[redacted]	B4	Peggy Barnhill
B4	Mary Ann Laslo		

VOL. 3
NR II

Final Edition

TABLE OF CONTENTS

On Saying Good-bye

For your warm reception of our
humble offerings....
Ten Thousand thanks.

For your steady support to
all our efforts....
A Million happinesses.

On severing such a close
liaison............
Quintillion sorrows.

Mink.

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

PROFILE OF A RATHBONE

by Joe Reid, B43

[redacted]

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

[redacted]

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

[redacted]

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

[redacted]

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

[redacted]

[redacted]

割猪草

下学了，
割猪草，
草儿绿，
味道好；
猪爱吃，
又长膘，
饲养员，
点头笑：
说咱红小兵觉悟高。

刘景林诗
赵广德画

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

THE CHINESE [redacted]: INFORMATION ALMOST LOST

by George Newhouse, B21

[redacted]

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

[redacted]

[redacted]

The problems encountered [redacted] are another instance of the age-old human tendency to reject something new, especially when there is no precedent. This tendency frustrates analysts who discover new and unusual information regarding their target country. Because people become so involved with past experiences, new ideas, new solutions and new methods are subject to much suspicion, often resulting in the loss of valuable information to the intelligence community. To avoid these potential losses every analyst and supervisor should make it a personal policy to evaluate new ideas, solutions and methods with an open mind. To paraphrase George Bernard Shaw, we should dream of things that never were and ask, why not?

THE PROFESSIONALIZATION OF A SUPER LINGUIST

YOUR SAY ENGLISH FIRSTLY! OR DO MY TRANSLATIONS READ LIKE THAT?

by John J. Mollick, B25

Have you ever wondered what kind of impression you make on someone whose native tongue is different from your own when you try to demonstrate your "profound" knowledge of his language? Through the years I have gathered a file of erroneous Chinese-to-English translations by non-English translators. The following unexpurgated examples, while humorous, might serve as a reminder that middling knowledge of a foreign language does not a polished translator make.

> I have been stolen on my way to the hospital and now in a very embarrass condition.
>
> Younger brother committed suicide by drowning himself to death in the river. That's the fact.
>
> Try as you can to put the personnel on the way to here as earlier as you can do.
>
> He wanted to quit his job for coming back to his native place. "Someone are trying to destroy me," he explained.
>
> I am sick, but I have not been admitted as in-patient to any hospital, so I have to liver and treat my disease in the hotel.
>
> I want to spend three more days to pull out and fill up my teeth. Inform if you approve.
>
> Dear you say English very good too. Your say English too very fine. Your say English firstly.

Tied up in my wife's unchastity, I can't return to unit as scheduled.

The division has provided us with the yarns-spinning workers.

Being treated with torture by your sister-in-law, your younger brother has come to my house and boarding with us a few days.

Not allowed to be discharged from the hospital where he received medical treatment because he was unable to pay the bill, he asked his truck in another city to mail him money.

Sir as I feel urgent please allow me to visit your country.

I'm seized with illness very seriously. If you are concerned, remit money at once; otherwise, leave me alone.

My son, who have been studied for several years at your institute, has failed in the examination because of effortless.

A man from your unit was stolen on leave. He is now at your station for he stole others.

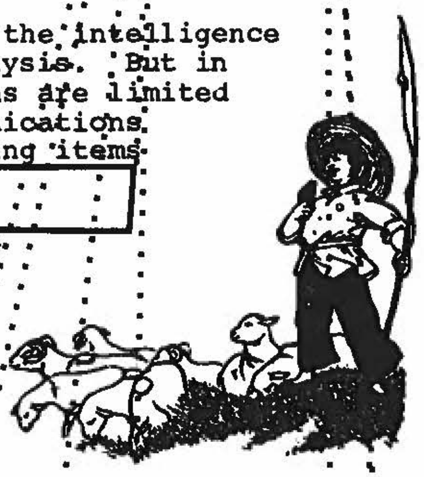
Seminar participants include professors from two universities. Their speak English ability weak.

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

LAUNDRY BAGS, BASKETBALL, HOG RAISING AND [redacted]

by Paul Savageaux, B21

Much has been said and can be said for the intelligence we glean from traffic analysis and cryptanalysis. But in those instances where military communications are limited or where the effective application of communications security exists, other intelligence--producing items must be exploited. [redacted] represent an exploitable item which provides order-of-battle intelligence. Practically all [redacted] information is obtained from civil communications and collateral sources.



[redacted] their use as part of the addresses in messages sent in civil communications; designate a unit or organization [redacted] The Chinese refer to the [redacted]

Collateral sources such as newspapers, radio broadcasts, and defector reports many times provide the initial and sometimes the only reference to [redacted] Such a reference with accompanying information is often the key to unit identification. [redacted] have been reported as appearing on a laundry bag with the [redacted] also printed on it, on the shirts of basketball teams, and in a photograph of a silk banner which contained [redacted] embroidered on it. Each of these were the first indication of the [redacted]

Analysis of plaintext Standard Telegraphic Code (STC) civil communications messages which contain [redacted] yields [redacted]

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

[redacted] provide a valuable means for maintaining continuity on unit locations.

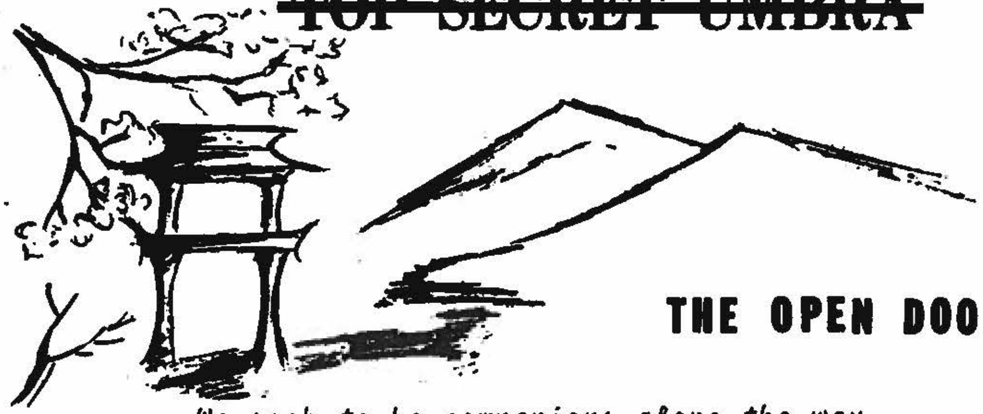
[redacted]

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

[redacted]

****

The camel even when
mangy, bears the burden
of many asses.
......Burmese proverb



THE OPEN DOOR

We seek to be companions along the way.
The lantern which we carry is not ours.
    The spirit which we share is contagious thought;
    The knowledge which we gain, an illuminating torch
And all who seek may perceive and learn.

-The Concept of Dragon Seeds

GEOPOLITICAL TIC/TAC/TOE IN THE INDIAN OCEAN

by Bee Kennard,C522

Tic-Tac-Toe and Geopolitics are universal games everybody plays. A world map neatly squared by latitudes and longitudes is the global board which the contestants continually fill with X's and O's. There is the local contest between adjoining countries, the middle game involving the big powers with the locals, and the top level international game among the big powers played for strategic stakes. By combining the two games, the information analyst can see what's happening and where the action is. Since superpower rivalry has just begun in the Indian Ocean, that fluid situation affords an ideal target to demonstrate Geopolitical Tic/Tac/Toe.

Play by Play Description

First, let's start with a calendar of events. The X's represent the political and military offensive moves, and the O's the defensive ones. The plays are then broken down by the game level upon which they are played. Since the undeveloped littoral and hinterland states have neither the desire nor capability of dominating the Indian Ocean, our sample model is limited to India, Australia and those islands and countries linked to the big powers. Due to technical difficulties beyond our control, the following tic/tac/toe game cannot be brought to you in 3D-living color. The split screen and a few winning plays have been selected for this abridged version.

Gamenates on Low and Middle Levels

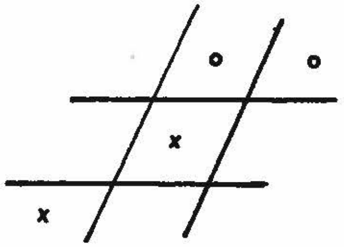
Gamenote No. 1: This mid-ocean shot shows that the first player has the advantage. The US won on the middle level by taking the center block on the opening play. The rule of thumb is: first player wins if he takes the center block and the second player doesn't take a corner. If the second player takes a corner, the game ends in a draw.

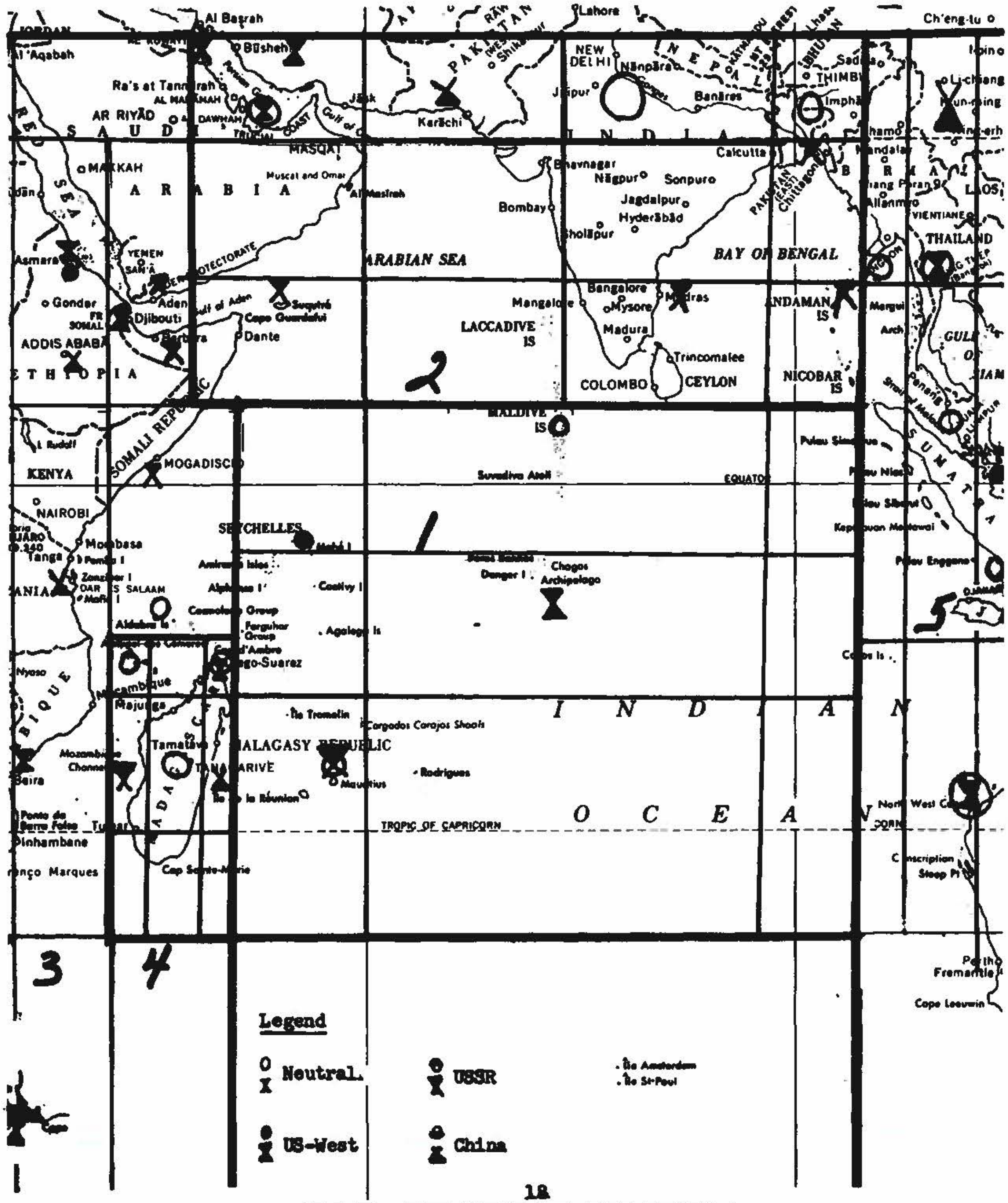
Gamenote No. 2: The Soviet move into the northwest quadrant of the Indian Ocean execplifies the draw game. From that area alone the USSR is within striking distance of Poseidon missiles launched from Polaris submarines. If the USSR can secure a base in the northeast quadrant, China comes under a Soviet ICBM threat.

Gamenote No. 3: With acquistion of the Somalia base, the Soviets are in position to score down the East African coast. If South Africa can moor the US to the Cape of Good Hope, then the US can control the southern entrance to the Indian Ocean. In this situation, the rule of thumb is: if both players play the corners, the first player wins who takes the center. Here the 3/T game switches from the offensive to the defensive.

Gamenote No. 4: Madagascar is an historic focal point in naval strategy and it is coming loose. As the defensive center, the third player can block a big power winning play but not sucesses on the outer fringe. Strategically, the center is the one that counts but half a game is better than none.

Gamenote No. 5: If the third player occupies the center block and plays the inbetween spaces, he can break up any scoring attempts by the big corner powers. The Southeast Asia move to neutralize the Strait of Malacca is essentially a no-win strategy but a tie game is often the best solution regionally and internationally.




Al Basrah
Būshehr
Lahore
Ch'eng-tu
JORDAN
Al 'Aqabah
Ra's at Tannurah
AL MANAMAH
DAWHAH
TRUCIAL COAST
Gulf of Oman
Jāsk
Karāchi
PAKISTAN (WEST)
Shikarpur
NEW DELHI
Nānpāra
Jaipur
Banāres
NEPAL
KATHMANDU
Lhasa
BHUTAN
THIMBU
Sadiya
Imphāl
Li-chiang
Kun-ming
Mo-chiang
Bhamo
AR RIYĀD
SAUDI ARABIA
MASQAT
Muscat and Oman
Al Masirah
RED SEA
MAKKAH
INDIA
Calcutta
Bhavnagar
Nāgpur
Sonpuro
Jagdalpur
Hyderābād
Bombay
Sholāpur
PAKISTAN (EAST)
Chittagong
Mandalay
BURMA
Lang Prabang
Allanmyo
LAOS
VIENTIANE
THAILAND
Rangoon
KRUNG THEP (Bangkok)
Asmara
YEMEN
SAN'A
ADEN PROTECTORATE
ARABIAN SEA
BAY OF BENGAL
Gondar
Aden
Gulf of Aden
Suqutrá
Cape Guardafui
Mangalore
Bangalore
Mysore
Madras
ANDAMAN IS
Mergui
Arch
FR SOMAL
Djibouti
Berbera
Dante
LACCADIVE IS
Madura
Trincomalee
GULF OF SIAM
ADDIS ABABA
ETHIOPIA
COLOMBO
CEYLON
NICOBAR IS
Penang
Strait of Malacca
KUALA LUMPUR
MALDIVE IS
SOMALI REPUBLIC
L. Rudolf
Pulau Simeulue
SUMATRA
KENYA
MOGADISCIO
Suvadiva Atoll
EQUATOR
Pulau Nias
NAIROBI
Pulau Siberut
Kepulauan Mentawai
KILIMANJARO 19,340
Mombasa
SEYCHELLES
Mahé I
Pemba I
Tanga
Amirante Isles
Salomon Islands
Danger I
Chagos Archipelago
Pulau Enggano
TANZANIA
Zanzibar I
DAR ES SALAAM
Mafia I
Alphonse I
Coetivy I
Cosmoledo Group
Aldabra Is
Farquhar Group
Agalega Is
DJAKARTA
Comoro Is
Cap d'Ambre
Diégo-Suarez
Cocos Is
Nyasa
MOZAMBIQUE
Moçambique
Majunga
Île Tromelin
Cargados Carajos Shoals
INDIAN OCEAN
Tamatave
MALAGASY REPUBLIC
TANANARIVE
Mozambique Channel
Beira
MADAGASCAR
Rodrigues
Mauritius
Île de la Réunion
North West Cape
Ponta da Barra Falsa
Tulear
TROPIC OF CAPRICORN
CORN
Inhambane
Lourenço Marques
Cap Sainte-Marie
Conception
Steep Pt
Perth
Fremantle
Cape Leeuwin
2
1
5
3
4
Legend
Neutral.
USSR
US-West
China
Île Amsterdam
Île St-Paul

Low Toe

O	Maldives becomes independent republic; Britian retains Gan airfield.	26 July 65
●	Seychelles and dependencies form new colony named British Indian Ocean Territory.	10 Nov 65
O	Mauritius becomes independent.	12 Mar 68
X	US plans to build radio and aid facility on Diego Garcia.	Dec 70
O	Bangladesh achieves independence.	Dec 71
O	Australia requests modification of US agreements re communications sites.	June 73
X	India and Australia to promote regional cooperation in Indian Ocean.	June 73
O	Comorro Islands to become independent.	June 73
O	Madagascar withdraws from franc zone; French troops to withdraw by 1 Sept 73.	June 73
O	Madagascar bars visit by four US destroyers.	27 Dec 73
O	New Zealand Prine Minister visits India; disapproves large foreign naval presence in IO.	28 Dec 73
X	Portugal offers US a port in East Africa.	26 Jan 74
X	France to strengthen naval presence in IO.	8 Feb 74
O	Australia, New Zealand and Indonesia oppose Anglo-American agreement to expand Diego Garcia	8 Feb 74
O	Magagascar denounces Anglo-American agreement.	8 Feb 74
X	India sends protest notes to US and Britain.	11 Feb 74

Middle Tac

X Australia-US agreement to establish naval communications site at North West Cape. May 62- May 63

X Goodwill visit to India by Commander of Soviet Pacific Fleet Mar 68

X Mauritius grants landing and docking rights to USSR. July 70

O India opposed to establishment of naval bases in IO. Nov 70

X Soviet offer to build submarine base in Andaman Islands. Mar 71

X India-USSR 20 year treaty of friendship, peace and cooperation. 9 Aug 71

X Soviet Defense Minister visits Somalia. Feb 72

X Soviet salvage fleet begins work in port of Chittagong. Apr 72

X Diego Garcia becomes operational. Mar 73

X Soviet airfield and longrange communications base set up in Somalia. Apr 73

O Bahrain orders US Navy to leave dock facilities. 29 Oct 73

X USSR formally requests standing port facilities in India. 20 Nov 73

X Mauritius signs agreement with USSR on aircraft landing rights. 23 Nov 73

X Brezhnev visits India. Soviet arms aid pledged. 26-30 Nov 73

X USSR seeks renewal of salvage contract with Bangladesh. 19 Dec 73

X China-Ethiopia establish air link; China offers to provide arms. Dec 73

O US-Australia agree to operate North West Cape jointly. 10 Jan 74

⧗ China-Madagascar sign economic, technical and trade agreement. 18 Jan 74

⧗ Soviet Foreign Affairs bureau chief visits Tanarive. 1 Feb 74

⧗ China-Pakistan agree to build SAMs. 21 Jan 74

● Kagnew communications base to close 30 June 74. Feb 74

⊖ Australia rejects Soviet request to build joint satellite tracking station. 10 Apr 74

⧗ South African Commander in Chief visits US privately. 7 May 74

<u>Top Tic</u>

● Soviet UNGA proposal Indian Ocean be declared nuclear free zone. 7 Dec 64

⧗ Soviet warships visit Indian Ocean ports. Mar-Nov 68

⧗ Soviet naval visits increase. 1969-70

● Britain announces withdrawal East of Suez by end 71. Jan 69

○ Lusaka resolution of nonaligned countries to keep IO Zone of Peace. Sept 70

⧗ Commonwealth Head of Government conference in Singapore to consider Soviet naval threat in IO. Jan 71

● US contemplating denuclearization proposal re IO to USSR. Apr 71

● Brezhnev calls for curtailment of cruises by navies in distant waters. June 71

○ Southeast Asia declares region Zone of Peace, Freedom and Neutrality. 27 Nov 71

⧗ US strike carrier Enterprise enters Bay of Bengal during Indo-Pakistani war. US intends to send naval forces into IO from time to time. 13 Dec 71

○ UNGA resolution declaring IO Zone of Peace. Resolution sponsored by Ceylon calls for complete demilitarization. China endorses resolution; US and USSR abstain. 16 Dec 71

● US-USSR discuss how to avoid naval arms race in IO. Tacit agreement to limit bases. 1971-72

⧗ NATO announces Britain and Netherlands to conduct patrols in IO. Dec 72

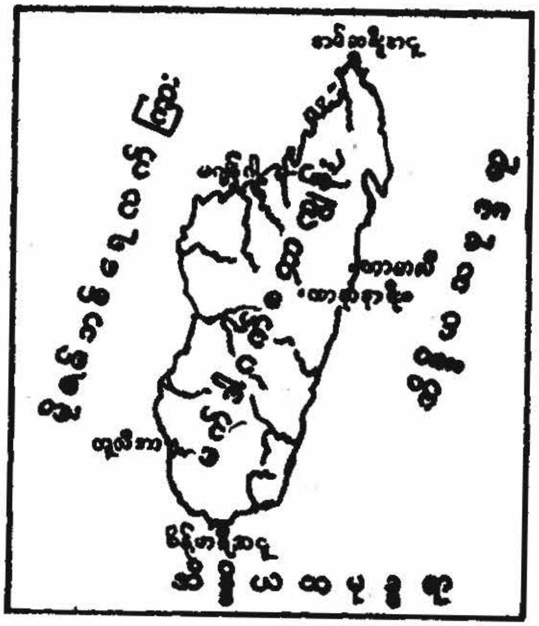
⧗ US sends naval task force into Indian Ocean 29 Oct 73

⧗ US Navy to visit IO on a more frequent and regular basis. 30 Nov 73

- Anglo-American agreement to expand Diego Garcia communications base into a modest support facility.
  5 Feb 74

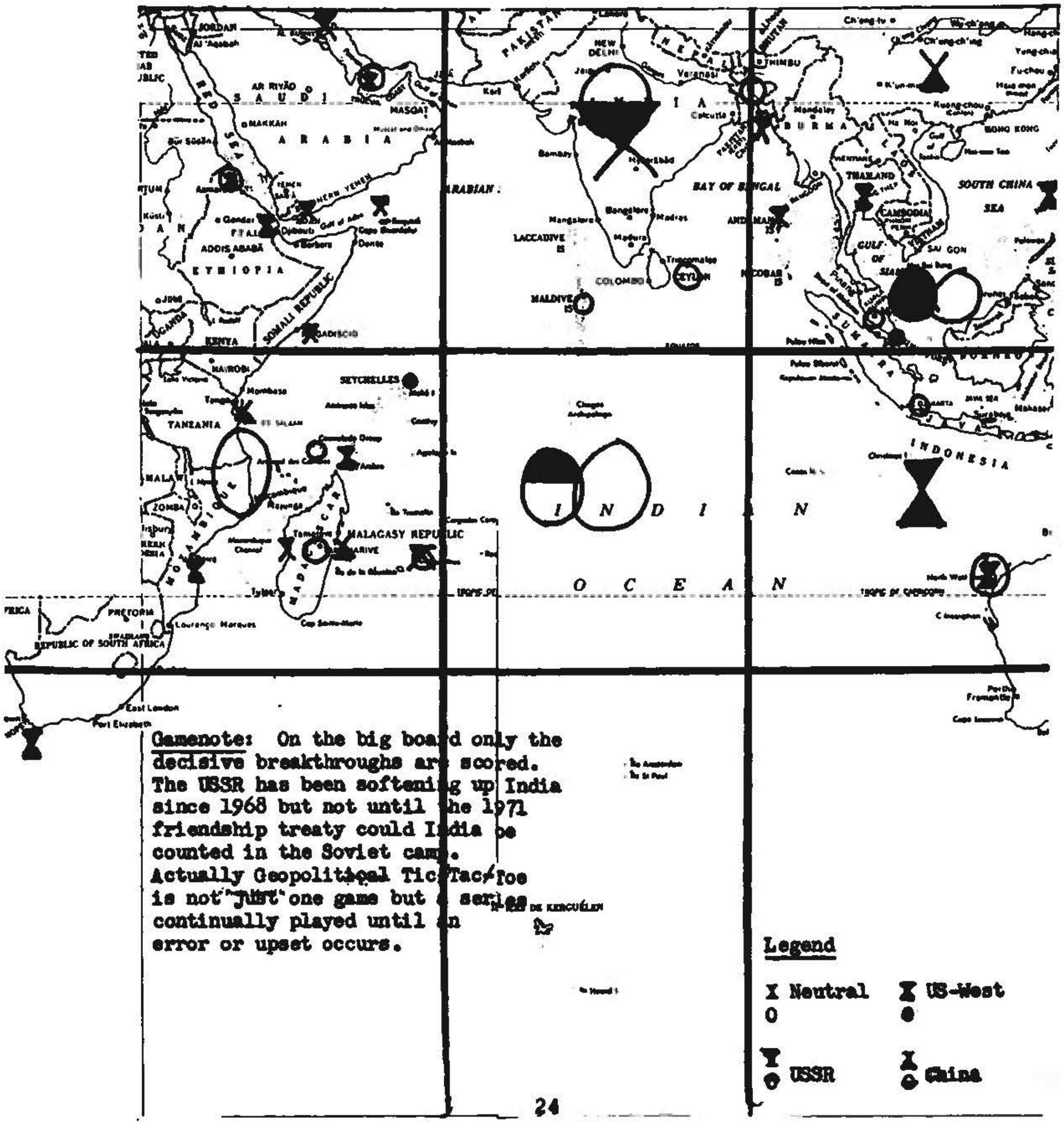
- USSR attacks projected US naval base as "dangerous to peace." Urges IO countries to regard it as a "direct threat to their security."
  27 Feb 74

- US carrier task force withdrawn from IO.
  23 Apr 74



3/T Formation

Next, let's take Top Tic, Middle Tac and Low Toe and superimpose them on a map of the Indian Ocean.



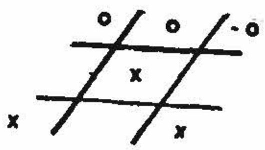
Gamenote: On the big board only the **decisive** breakthroughs are scored. The USSR has been softening up India since 1968 but not until the 1971 friendship treaty could India be counted in the Soviet camp. Actually Geopolitical Tic/Tac/Toe is not "just" one game but a series continually played until an error or upset occurs.

Monday Morning

Now the analyst can actually see how the geopolitical game shapes up in the Indian Ocean. On Middle Tac the US has scored a diagonal tic/tac/toe with communications sites from Ethiopia to Diego Garcia to Australia. Likewise the USSR got in on the ground floor at the US and together with the neutralists was winning the international political game. However, the US decision to expand Diego Garcia into a support base has dramatically changed the strategic outlook in the Indian Ocean. The deployment of a US naval task force to the Persian Gulf during the Middle East confrontation forcibly reminded the Soviets of the SLBM threat from the Indian Ocean and served notice of US intentions to protect the oil life-lines to Japan and NATO.

South Africa is attempting to cash in on its strategic gateway astride the oil lanes from the Indian Ocean. A western military alliance would enhance its reputation whereas Southeast Asia is trying to get out from under and into the neutralist camp.

Neutralist efforts to preserve the neutral character of the Indian Ocean come too little and too late. Big power rivalry to fill the vacuum left by British withdrawal East of Suez is well under way. In a word, the Indian Ocean is up for superpower grabs. However, rules and predictions seldom allow for human error so upsets are frequent in the balance of power contest. If at first you don't succeed in geopolitics, try patience and persistence.



xooox

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

DOING THE TWIST OR FORMULAS FOR FINDING THE EXPECTED NUMBER OF CANONICALLY TRANSFORMED HITS (TRANSPOSED GROUPS) WITHIN A GIVEN SAMPLE

by Mary Ann Laslo, B43

[redacted]

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

[redacted]

[redacted]

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

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

[redacted]

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

~~TOP SECRET UMBRA~~

[redacted]

~~TOP SECRET UMBRA~~

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

[redacted]

東洋의 山

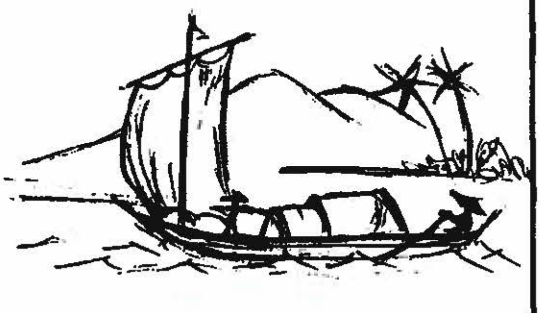
이한직

비쩍 마른 어깨가
抗議하는양 날카로운 것은
告發않고는 못참는
애달픈 天稟을 타고난 까닭일께
다
激한 噴火의 記憶을 지녔다
그때는 어린대로 심히 怒해
볼수도 있었기 대문이다.
植物들은 해마다 헛되히
뿌리를 박았으나
끝내 森林은 이루지못하였다
지나치게 悽慘함을 겪고
나면
오히려 이렇게도 마음고요
해지는 것알까

THE HILL OF THE ORIENT

YI HAN-JIK

THAT MY BONY SHOULDERS ARE SHARP
AS IF IN PROTEST
PERHAPS IS FROM THAT IMPATIENT
TEMPER OF MINE
WHICH SEES AND MUST ACCUSE.
I CARRY MEMORIES OF VOLCANIC
VIOLENCE;
FOR THEN I WAS FREE TO BE FURIOUS.
MY PLANTS HAD ROOTS, IN VAIN,
EVERY YEAR
AND NEVER GREW TO BE A FOREST.
IS IT BECAUSE I HAVE WALKED
THROUGH TOO MANY CRUELTIES
THAT I AM IN SUCH QUIETUDE?
I HAVE NOW NOTHING TO INSIST UPON.



이제는 固執 하여야 할 아무
　主張 도 없다

지금 山기슭에 "부주카" 砲가
　震動 하고
共産主義者 들이 낯설은
　外國 말로 喊聲 을
　올린다
구리고 實로 믿을 수 없을 만큼
　손쉽게
쓰러져 죽은 善意의 사람들
아 그러나 그 무엇이 나의 이고요
　함을
깨틀일 수 있으리오
눈을 꼭 감은 채
나의 表情은 그대로 얼어붙었나
　보다
微笑 마저 잊어 버린
나는 東洋의 山이다

AT THE MOMENT
THE HILL-SIDES SHAKE FROM THE
　BAZOOKAS;
THE COMMUNISTS RAISE SHOUTING
　IN ALIEN TONGUES;
AND THOSE GOOD-WILLED PEOPLE
　HAVE FALLEN SO EASILY
THAT I CAN HARDLY BELIEVE IT.
BUT, NOTHING CAN DISTURB ME OR
　MY QUIET NOW.
WITH TIGHT CLOSED EYES,
THE ICE OF MY EXPRESSION FREEZES
　HARD.
I, WHO EVEN HAVE FORGOTTEN HOW
　TO SMILE,
AM THE HILL OF THE ORIENT.

TRANSLATED BY KIM JONG-GIL

道

THE FABLE OF THE PROFESSIONAL LINGUIST

By Dan Buckley B32

Once upon a time in the sleepy country of NSALAND, near Washington, D.C., a strange animal was born. Now, in many countries this event would have been newsworthy, perhaps even reportable in a WAR or other weekly, but this mother had given birth to such strange animals in the past that little attention was paid and the new arrival, called professional linguist, was more or less ignored and allowed to grow or not grow as he chose.

Being an aggressive animal, professional linguist chose to grow and discovered much to his liking that he flourished on various colored pieces of paper called traffic. Also much to his liking, he found that supervisors truly appreciated the way he devoured the traffic feed, routed it through his internal circuitry and regurgitated it in some form comprehensible to those animals different from him, who almost always were larger than he. But he did grow. From seven to nine he went, then to eleven, and lo, even to twelve. He truly realized his nature by this time and in that realization he also came to know that the animals larger than he did not fully understand him. Oddly, he thought, they often kept on growing while he had stopped. As the years passed and he grew no more, he wondered about this mysterious afflication that had befallen him. Examined by all sorts of other professionals, there appeared to be nothing lacking in his external forces: performance appraisals, awards, certification, etc. But nothing would make him grow. He ate more traffic, wrote more translations, fissioned another certification, and was adored by all. Nothing! Then one day, one of the larger animals asked him: "Why do you not become a different kind of animal. Everyone knows that linguists are bright and skilled, especially professional linguists, but they are always so small. If you want to become a larger animal, you must certainly start by becoming a different animal."

Professional linguist was crushed. It had simply never occurred to him that the mysterious afflication haunting him was the nature of the beast itself. He could not believe it and he went in search of professional linguists who had grown larger than 12. After many months of searching, he found one who had grown to fifteen and was considered to be a veritable wizard. The wizard listened to the dilemna of the smaller professional linguist and sympathized with him. In the end, he admitted that very few professional linguists had grown greater than twelve while eating traffic. More important, the wizard explained the process of metamorphosis to professional linguist. It was simple: he had only to stop eating traffic, to leave the eating of traffic to smaller linguists and he would grow. His diet would consist largely of timecards, performance appraisals, activity reports, and hinkel ham sandwiches. Except for the ham sandwiches, he found the fare not nearly so tasty as the multicolored paper traffic feed, but it was indeed more nourishing. Very soon he grew to thirteen and his hopes for further growth were bright.

Much to his delight, he found that he was not alone as a metamorphosized linguist, as he thought he surely would be. NSALAND was literally crawling with them and along with them, he gourged himself with hinkle ham and said words like "management" and "interface", which he did not truly understand. But no matter, because he no longer understood the language with which he was born either and it seemed entirely appropriate.

The moral of this fable is: Wet birds don't fly at night (which makes about as much sense).

****

"Chairman," said Mrs. Mao,
"You sigh and you pucker your brow,
Your fingers are weaving like knots --
You're having, perhaps, second thoughts?"

...Johns Hopkins Magazine
June 1974

SO WHAT WOULD YOU EXPECT?

by Jane E. Dunn, B4 TDT

You are a manager among whose newly acquired responsibilities is the production of intelligence information from encrypted messages of a SIGINT target. Your personal background is firmly in T/A and reporting, and you have always felt that CA was an esoteric art that an outsider could not really appreciate. Now you must sit in judgment of people and operations in that "foreign" field. What should you expect of a crypt effort? More pertinently, what should you expect of the cryppies involved in it? If your deputy is an experienced, professional cryptanalyst, you have some breathing space, but the responsibility is still yours. Here are some thoughts from one professional cryptanalyst and erstwhile manager which may help.

The good crypt effort, whether manned by one or one hundred people, is marked by a "professional" outlook. Its operations are oderly, comprehensive, and documented. Its members characteristically use the scientific method of systematic pursuit of knowledge yet are flexible enough to allow for and to profit from the intuitive leaps that sometimes bring solutions. The effort progresses as far along the path of diagnosis, solution, exploitation as the resistance of the systems and the human and machine resources to attack them will permit. Individually and collectively, the crypt group keeps itself informed about advances in cryptanalysis against other targets through reading technical publications, participating in professional assemblies and conferences, and obtaining advanced training to increase and sharpen skills both in crypt and in related SIGINT disciplines. The group and its members keep in close touch with the non-crypt aspects of its own its own target problem, making sure that the exchange of information is two-way.

An indispensible part of the professional and scientific effort--in crypt as in any other technical discipline--is documentation. The manager should expect that procedures and results will be put on the record. Formal or informal reports published in the appropriate technical series are minimal requirements. Publication in the NSA Technical Journal will give wider dissemination to good ideas and may bring the author and his problem the bonus of professional recognition outside his immediate area. Encourage technical reporting.

With the "professional outlook" established as a necessary base, what about the work the cryppies do? How does a non-cryptanalyst judge cryptanalysis? Perhaps the manager cannot expect to penetrate the interdisciplinary wall, but some aspects of the actual work can be assessed by an outsider. Good marks go to goal-oriented work--organizational goals, that is--rather than to work which only satisfies the personal likes of the individuals doing it. If the work can meet both objectives, so much the better. You should look for attributes such as initiative, imagination, innovation, and enthusiasm tempered by practical good judgment about potential results. There should be an evident willingness to learn about and to use modern methods and tools such as computers and to maintain and improve individual technical skills.

Technical reports and records, published and unpublished, formal or informal, can let you see what is going on and can help you to evaluate the crypt effort, its directions, and prospects as well as its people. Read them.

The cryppie knows he has reached a solution when the system "reads." The manager has no such definite measure in evaluating a crypt effort. Perhaps these few ideas can provide a sort of check list or starting point to help him arrive at a reliable judgment about this part of his responsibilities.

— • —

Here are some thoughts on the kinds of documentation a cryptanalyst should keep. There will be some omissions depending on whether the analyst is working on an exploitation or a research problem, on a bookbreaking or a diagnosis problem.

A cryptanalyst is a record keeper and classifier, and he owes it to his employer to keep those records outside his own head and in such form, content, and volume as will be accessible and useful to contemporary and future analysts and managers.

1. System descriptions (encrypt versions), samples of traffic, decrypts, product.

2. Key recoveries, code recoveries--up to date.

3. Oddities and cryptocharacteristics by system, target, correspondent.

4. Plaintext logs and indexes.

5. Traffic counts and logs.

6. Descriptions of work done--approach, procedures (including computer program names, descriptions, and output), results.

7. CIP (or whatever it is now) documents; lists of isologs and possible depths.

8. Pertinent TA and collateral information; captured cryptomaterials' structure and use.

9. Pertinent information about predecessor and contemporary systems of the same or related targets.

10. Translated decrypts of particular intelligence interest.

11. Proper names encountered; target's names for institutions, practices, organizations, and materials.

12. Crib lists.

13. Notes to the next comer--"try these first".

Not to forget when wrapping up a problem to prepare a vital records package (on microfilm probably) including a technical report.

The official technical records such as system descriptions, traffic counts, TEXTA information, should be in the official vehicles for such records--for crypt, the Crypt Status Report--and in such published documents as crypt identification guides, etc. But they should also be part of the "package" the working cryppie keeps for his own problem. CI information should be published in the appropriate product series. It is all part and parcel of the analyst's not hugging knowledge to his breast as though it might diminish his stature if someone else knew about his problem, progress, or techniques. He needs to get it on the record so others can make use of it.

****

SAYINGS OF THE SAGES :

The real fault is to have faults and not try to amend them.

Pale ink is better than the most retentive memory.

To go beyond is as bad as to fall short.

Knowledge is boundless but the capacity of one man is limited.

An inch of time is worth more than a foot of jade.

Settle one difficulty, and you keep a hundred others away.

過猶不及

COMING ATTRACTIONS:

Statistics on Chinese Plain Text

BACKGROUND

Over one millon characters of Chinese plain text represented as CTC (Chinese Telegraphic Code) groups and recorded on magnetic tape were given to NSA [redacted]. The CTC groups were translated to STC (Standard Telegraphic Code), and recoded from the Honeywell Tip Top to the Burroughs 6700, the 6700 providing quick turn-around on debug programs.

The study of this file was undertaken for two main reasons:

a. To support cryptanalysis [redacted]

b. To provide Chinese linguistic information for language training at NSA, the CETA (Chinese-English Translation Assistance) Groups, and [redacted]

A committee was formed by Ken Cohen, then in B45, to design the programs for the statistical analysis of this huge data bank. The committee members were:

B03 Linguist, Norman Wild
P15 Crypto-mathematician, Catherine Krafft
B43 Cryptanalyst/mathematician, Mary Ann Laslo (x3755s for general information).
B42 Programmer, Alton Gowen
B42 Programmer, Michael Cavanaugh
B42 Programmer, Richard Neal (x4823s for program information)

In addition, Dave Claybrook, B4TDLA, provided the Chinese graphic characters for the runs; and Ed Stoops, B44, and Elsie Flemming (now retired), B441 provided general English meanings for the STC groups and helped to proofread the output listings.

It was decided to publish the output statistics in four parts:

Part I	Statistics on STC Data-Digital (Tetranomic) Form.
Part II	[redacted]
Part III	Statistics on STC Data-Literal (trigraphic) Form.
Part IV	[redacted]

Only parts of Part I (those of linguistic interest) will be distributed outside NSA.

PL 86-36/50 USC 36C

STATISTICAL STUDY, Part I

The [redacted] STC File Statistical Study, Part I, is almost completed, and should be available sometime in June 1974. Part I, "Statistics on Digital (Tetranomic) STC" will be published as a B441 Working Aid, and will contain the following information.

1. MONOMES- each of the four positions-in-group and all four positions combined:

a. frequency distribution
b. percentage
c. repeat rate
d. gamma I.C.
e. total sample size

2. DINOMES

a. dinomic frequency distribution
b. percentages
c. repeat rate
d. chi square statistic
e. gamma I.C.
f. total sample sizes for the dinomes:

A, B)
A, C)
A, D) within group
B, C) studies
B, D)
C, D)

A, A1)
B, A1)
C, A1) Across group studies
D, A1)

A, B, C, and D are the four positions of an STC group, and A1, B1, C1, and D1 are the four positions of the group immediately following that group.

3. TRINOMES

a. inverse frequency listing of the 100 highest frequency trinomes
b. repeat rates
c. chi-squared statistics
d. total sample sizes

The above are given for each of the following trinomes:

A,B,C)
A,B,D) within
A,C,D) group studies
B,C,D)

C,D,A1) between group
D,A1,B1) studies

4. TETRANOMES Across Group

The following are given for the tetranome A, B, A1, B1:

a. inverse frequency listing of the highest 100 tetranomes
b. repeat rate
c. chi-squared statistics
d. total sample sizes

5. MONOGROUPS

a. A listing of monogroups comprising 50% of the total sample, sorted in inverse frequency order
b. The same as above, except sorted by telecode number
c. Statistics:

monogroup frequencies
percentages
total percentage displayed
unique monogroups displayed
unique monogroups processed
total of frequencies displayed
total sample size

*d. A complete inverse frequency listing of all unique monogroups in the entire sample, together with:

the frequency distribution
percentage
the cumulative percentage
the Chinese graphic characters
number of unique monogroups
repeat rate
total frequency displayed
total number of unique groups displayed

*e. The same as above, only sorted by telecode number

6. DIGROUP STUDIES

a. A listing of chained digroups comprising 15% of the sample, sorted in inverse frequency order
b. The same as above, but sorted by telecode number
c. Statistics:

frequency distribution
percentage
Chinese graphic characters
general English meanings

repeat rate
chi square statistic
number of unique digroups displayed
sample size

*d. An inverse frequency listing of all digroups occur occurring three or more times, using the entire sample as the data base. Also given are the frequencies and percentages.

*e. The same as above, but sorted by telecode number.

7. TRIGROUP STUDIES

a. A listing of chained trigroups comprising 5% of the sample, sorted in inverse frequency order.
b. Same as above, but sorted by telecode number.
c. Statistics:
frequency distribution
percentage
repeat rate
unique trigroups displayed
total frequency displayed
sample size

*d. An inverse frequency sort of trigroups occurring two or more times in the entire sample, with the frequency and percentage.

*e. A telecode number sort of the above.

*8. SENTENCE BEGINNINGS AND ENDINGS

a. An inverse frequency listing of 75% of those monogroups appearing at the beginning of sentences

Also given: the frequency distribution
percentages
Chinese graphic characters
general English meaning
total frequency displayed
total unique groups displayed

b. Same as above, but with sentence endings.

*9. PUNCTUATION

a. Total number of commas in entire file and percentage.

PL 86-36/50 USC 3605

b. Total number of periods in entire file and percentage.

c. The new total sample size, including punctuation (not included in other runs, because punctuation is represented by symbols rather than 4-digit groups).

10. 5-5 WINDOW INDEX

On each of the eight categories individually.

The above statistics were developed both on the eight individual subject categories and on the entire file (ALL SUBJECTS), except where the * appears. The * indicates the statistics were done on the entire file only, and not on the individual categories.

George Sing, B4, has promised a large file of newspaper articles which will also be processed along these lines. This will add another dimension to the data base, making this project wider in scope.

[redacted] STC FILE DATA BASE

	Categories	Number of 4-Digit STC Groups Excluding Punctuation
1.	FICTION	537,122
	a. Drama	
	b. Literary Essays	
	c. Novels	
	d. Novellas	
	e. Short Stories	
2.	ESSAYS	135,911
	a. Biography	
	b. Literary Criticism	
	c. Educational Essays	
	d. Political Essays	
	e. Social Essays	
3.	HISTORY	60,579
	a. Sociology	
	b. Ancient History	
	c. Intellectual History	
	d. Modern History	
4.	COMMUNIST IDEOLOGY	104,996
5.	KMT IDEOLOGY	20,997

6.	LANGUAGE	
	a. Literary Policy	70.326
	b. Language and Rhetoric	
	c. Language Standardization	
7.	JOURNALISM	22,955
	a. Editorial Journalism	
	b. Reporting Journalism	
8.	PHILOSOPHY	44,027
	a. Philosophy	
	b. Literary Criticism	
9.	(LAW)	(5,000)
10.	(ARCHEOLOGY)	(2,800)
	ALL SUBJECTS (includes all of the above categories	1,003,194

The last two categories (law and archeology), were included in the ALL SUBJECTS runs, but omitted in the processing of individual categories because of the small volumes in the categories, and unusual subject content.

Therefore the data base represents 10 general subject categories, composed of 25 subcategories.

---- SO LONG! IT'S BEEN GOOD TO KNOW YOU.

By decree of Gen. Herbert E. Wolff, DDO, publication of *DRAGON SEEDS* will cease with this issue. We are grateful to all of you whose volunteer efforts made it a publication B could be proud of. Please submit future articles for publication to: CRYPTOLOG, P1.

***

---The B4TDT is looking for a general term which would describe the functions of a "meaning digit," "Ø-select system," and other devices which permit the user of a code or code chart to modify, change, truncate, expand or limit the meaning or plaintext value of a code group. Send your suggestion to Betty Dunn, B4TDT. If we get a good one, we will send it on to Mr. Callimahos for possible inclusion in the Basic Cryptologic Glossary.

***

---OMNIBUS

OMNIBUS is a network of computers being developed as an enhancement of the existing WARSAW system. The network will consist of a dual processor DEC System 10, and eleven or more PDP-11s. The DEC-10 will control the network and interface with other Agency computers through a PDP-11. Other PDP-11s will control the CRTs and GRAPHICS communications.

The dual processor DEC-10 configuration is currently comprised of 96K of core memory with paging hardware, one swapping drum, two discs and sixteen CRT terminals. Future expansion is expected to reach 256K of core, four drums and twelve discs.

Version 5.06A of the standard DEC-10 monitor is the current operating system. This is a time sharing monitor that provides service for up to 35 time sharing or batch users.

The PDP-11 systems in OMNIBUS are 16K minicomputers using the RSX-11A Operating System. This is a real time executive that can handle a multi-programming environment yet utilizes only 2-5K of core memory. Other major features of this system include modular design, fixed priority scheduling and time dependent task initiation.

For information concerning the OMNIBUS operating system contact Aaron Engel or Pete Wyatt, C433, X4286.

***

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

---Misplaced during departure from the TDLA, a small volume of poems in Korean with English translations. Please notify Minnie M. Kenny, x5078 if found.

***

---B CRYPT SEMINARS

To help us working analysts break out of our "target" boxes we plan an open-ended series of informal and informative technical seminars so that we can all learn more about B Group cryptosystems and operations. Each meeting will be an audience-participation, show-and-tell session of one fairly limited B crypt or crypt-related subject. It will be led by whoever knows most about the problem, usually the analyst who is now working it.

We will try to hold one seminar each month but will not bind ourselves to a rigid schedule.

The following subject have been suggested:

[redacted]

[redacted]

Crypt Documentation
Calligraphy

Suggestions of topics and group leaders are welcome at any time. Bill Mau of B43 has agreed to lead a session on [redacted] to start off the B crypt seminars. Time and place for the meeting will be announced later.

---The muezzin mooed, the tocsin tinkled, and the faithful flocked to the Call. Verily a select population! The now 235 Dundee members for the last 19 years have formed the hard core of soft-hearted, pliable, versatile technicians nurtured in the arcane mysteries of a noble art in the finest traditions of the giants of yesteryear. (Wa-we-woo, we were almost carried away there!) Eyes dimmed, if not from the ravages of time, at least from the emotional strain of our awesome responsibilities. But juubun is enough (in Japanese that is).

Wednesday, 12 June, was the Eighth Annual Reunion of the Dundee Society, held as usual in the Ballroom of the Fort Meade Officers Club. The festivities began at 1115 with convivial tinkling of glasses.

As was the Dundee custom, mystery guests of suitable noble birth and station, General Lew Allen Jr. and Benson K. Buffham, were present to receive Honorary Membership.

***

The Chinese word for 'crisis' contains two characters - one of them means 'opportunity'

危　机

***

---CACP Basic Requirement for a Computer Program

For a computer program to be accepted by the CACP either as meeting the basic requirement or for additional points:

1. It must serve a cryptologic purpose related to the cryptanalysis or exploitation of operational encrypted traffic.
2. It must work.
3. It must give evidence that the aspirant has a good appreciation of the role computers should play in supporting cryptologic activity.
4. It must demonstrate a professional attitude on the part of the aspirant by exhibiting a number of the functions generally incorporated in a computer program, by showing originality of purpose or technique, and by performing a complete task.

(Note: Originality, technique and a display of basic programming knowledge count more than amount of output, number of lines of coding and degree of operational usage. For instance full credit would be given to an original one-line APL program that printed "yes" or "no" on a one-shot pass if it accepted C/A data, wrung it out, tallied, tested and computed an important statistic. This is in contrast to a program which might serve a vital operational function by simply converting 26-letter sequences to sequences of L's and R's denoting the halves of a typewriter keyboard, but which certainly doesn't demonstrate professionalism.)

Programs written as exercises in programming courses are not acceptable. Compartmented programs will be accepted for evaluation.

***

---Teaching Opportunities

A note from Eliot Sohmer, Head of the Computer Science Department, E21, passes on the information that the National Ceyptologic School has some unique opportunities for professionals who wish to sharpen their skills by teaching.

What many NSA employees don't realize is that you *do not* have to be permanently employed at the School to teach. This presents an opportunity for an employee to teach in any area of his specialty.

If you think that you might be interested in teaching a class or running a seminar, call Jack Leonard, E1, x8027 or Eliot Sohmer, E21, X8555.

***

---PROFESSIONALIZATION NOTES NEW CRITERIA FOR CSAs

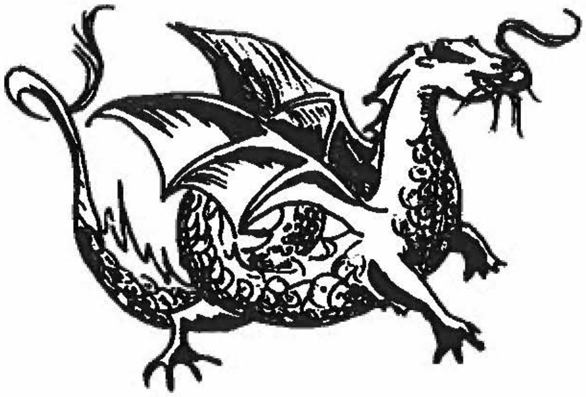
Have you heard that a New Criteria for Computer Systems Professionalization has been approved and published? It became effective 1 January 1974 and should have reached your element by the time you read this.

If you have not been certified as yet, it will affect you. If you submitted your PQR prior to 1 January 1974, you will be rated under the Old Criteria unless you make a request, in writing, to be rated under the New. Those rated under the Old Criteria will continue to maintain all the points awarded under the Old Criteria but will earn additional points and fall under the New Criteria effective 1 January 1975, if they have not been professionalized prior to that time. This grace period is covered in a memo that was approved by the CSCP and ADPS.

The general effect of the New Criteria is to require a technical paper from all aspirants (not just Interns) and to require the Interns to pass the same examination that all other aspirants must pass. It also places more emphasis on current training and computer related education, because this field is so dynamic that computers studied ten years ago are not nearly as relevant as computers studied today.

Detailed information can be obtained from the Data Systems Career Panel.

***



ASK THE DRAGON LADY

Dear Dragon Lady:

While we're still discussing the linguist at NSA, I feel a few words should be said about his training, especially where the minor tongues are concerned. In that regard, I'd like to pass on some points made by Prof. Carleton Hodge of Indiana University in a paper titled "Pedagogic Responses to Linguistic Stimuli" presented at the Georgetown Round Table. (March 1973).

Thorough cultural study should accompany the linguistic study of little-known languages.

Experiments have been conducted in which some students beginning the study of foreign languages were given drill in speaking from the beginning while others went through a "pre-speech phase" in which for eight weeks they developed only comprehension ability without attempting speech. It was found, that when the latter group was taught to speak, pronunciation, as well as comprehension, was better than that of the former group.

Fully structured texts are needed so that points of grammar are understood before they are used rather than explained afterward.

Robert F. Kreinheder

******

What can be done for the linguists?
Theirs is not gain, but loss,
For they only talk to each other
And nobody talks to the boss.

Anonymous (alias Marian Griggs)

Dear Dragon Lady:

In the issue dated March 1974, the article titled "B Signals Lab Capabilities and Mission" was erroneously listed as being written by Mr. Robert Earles. The article was originally written as a memorandum to be distributed down to the branch level throughout B. Somehow in the transformation from memorandum to "Dragon Seeds" article, the name of the correct drafter became somewhat of a mystery. So that the record might be set straight, the undersigned recognized the need for such an item, discussed the idea with the Deputy Chief of B43 and wrote the article as it appeared in your March 1974 issue

Donald K. Autry

****

"This wise man has indeed a healthy mind";
He sees an aberration as it is
And for that reason never will be ill."
-- Lao Tzu

****

Dear Dragon Lady:

Where can I get extra copies of the March 1974 issue of Dragon Seeds? Several of my G analyst friends would like copies of their own to use as RYE reference manuals.

Sonia Randall, H11

Dear Sonia:

Asking is receiving DL.

****

Dear Dragon Lady:

There should be some general diagnostic programs on the LODESTAR system.

Some interesting points:

Persons most familiar with the 6600-7600 systems will state that the inactive mode is <u>not</u> the most efficient way to use these computers.

And, at least 1/2 of our cryptanalysis (in B) depend upon general diagnostic programs rather than specialized or interactive type programs.

Anyway,there's nothing to stop individual users from putting the general diagnostic programs in their workspaces.

The RAPID programs are in bad shape, and rewriting the most frequently used of these in BETA will correct the errors, as well as make them available on Burroughs 6700 and the 7600.

When and if these programs are rewritten, it will be done in as interactive a way as possible to cut down on output and machine time. (Eg. BIGSTET format rather than STET)
So why not on LODESTAR and now?

Mary Ann Laslo

****

Dear Mary Ann:

Will forward your query to C for resolution.

D. L.

****

A special word of thanks to Brenda Collins, Jackie Haislip, Helen Ferrone, and Jan Sanderson *for their willing and able assistance in getting this last issue to press.*

EO 3.3b(3)
EO 3.3b(6)
PL 86-36/50 USC 3605

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

CONTRIBUTORS

DAN BUCKLEY has spent a year at [redacted] [redacted] and three months at [redacted] on language related assignments since his last appearance in DRAGON SEEDS (The Ground Zero Approach to Language Analysis, Volume II,Nr 1 March 1973). He was certified by the Language Career Panel in March 1969 and by the SRA Panel in February 1972. He is currently assigned to the North Vietnamese Air Defense problem in B32.

JANE (BETTY) DUNN'S connection with SIGINT dates back to WWII [redacted] and covers targets from Japanese Military to CHICOM [redacted] with stops along the way for work on [redacted] [redacted] European Satellite, and Vietnamese Communist cryptosystems. She holds a B.E. from Duquesne University and was prepared to teach French in Pennsylvania high schools before she was detoured to Arlington Hall. Betty is a certified cryptanalyst, a tutor for the CA Intern program, an E.E.O. counsellor, and most recently the Cryptanalysis Editor for the new magazine, Cryptolog. In the latest B reorganization, Betty was assigned to the B4 Technical Discipline Team.

BEE KENNARD, C522, graduated from the University of Texas with a B.A. in History and English. For seven years she served as an intelligence analyst with G2, U.S. Forces in Austria. In October 1959, she joined NSA and has since worked in the various area branches of C52. From 1967 to 1971, she worked with P2223 collocated information support group as the senior analyst on the Vietnam military problem. She is a professional Information Science Analyst and is currently writing articles on the new ideas and techniques in information services.

MARY ANN LASLO, B432, was graduated from Rosary Hill College, Buffalo, New York, in 1965, receiving a B.A. degree in Mathematics. She came to NSA in 1966 and entered the C/A Intern Program, which provided opportunities to work in A55, B45, G41, and G42. She received her certification as a mathematician in 1970 and as a cryptanalyst in 1973; and she has completed several requirements leading to certification as a crypto-mathematician. From 1969,

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

to 1973 Mrs. Laslo was assigned to G91, where she did independent cryptanalytic research on the Peoples Republic of China [redacted] and functioned as a consultant in mathematics and statistics at Division level. Mrs. Laslo is now chief of the Chinese High Grade Cryptanalysis Team in B432.

JOHN J. MOLLICK, B25, studied Mandarin Chinese at Yale University Institute of Far Eastern Languages in 1955-56 and then served as intercept operator, voice transcriber, and traffic analyst with the USAFSS in Korea until 1958. His NSA (and B) civilian service stretches from 1959 to the present, punctuated by an academic year (1966-67) of advanced Chinese area and language studies at the U.S. Foreign Service Institute in Taichung, Taiwan. Mr. Mollick is certified in the fields of Language (Chinese) and Special Research. He was a frequent contributor of Chinese language articles to the Quarterly Review for Linguists. His present position is Chief of the PRC Documentation and On-Line Processing Branch, B253.

GEORGE NEWHOUSE, B21, received his B.A. in Business Administration from the University of Maryland in 1970 and is now completing work for his M.B.A. at the University of Hawaii. Since he came on duty with the Agency in 1963, he has worked on various B problems as a traffic analyst and reporter. A certified Special Research Analyst and Traffic Analyst, George now serves as the technical rerepresentative at USM-3 in Okinawa.

JOE REID retired 30 June 1974, ending a SIGINT career that dates back to WWII when he was a U.S. Navy intercept operator. His assignments at NSA and predecessor agencies covered Soviet low-, medium-, and high-grade cryptosystems, and included 15 years experience on Soviet and Chinese Communist data systems.

PAUL SAVAGEAUX has worked in B21 since 1965, after having completed a tour as Intelligence Analyst at Pacific Army Headquarters in Honolulu the previous year. He spent eight years on the [redacted] problem and is currently assigned to B21's Term Reporting Team which is writing a history of the PLA [redacted]. Paul graduated from the University of Mas-achusetts in 1961. He is a certified Special Research Analyst.

GOOD BYE...