~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

2nd Issue 1992

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

P.L. 86-36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~CLASSIFIED BY NSA/CSSM 123-2~~

~~NOT RELEASABLE TO CONTRACTORS~~

CRYPTOLOG

Published by P05, Operations Directorate Intelligence Staff

VOL. XIX, No. 2 . . . . . 2nd Issue 1992

PUBLISHER . . . . . [redacted]

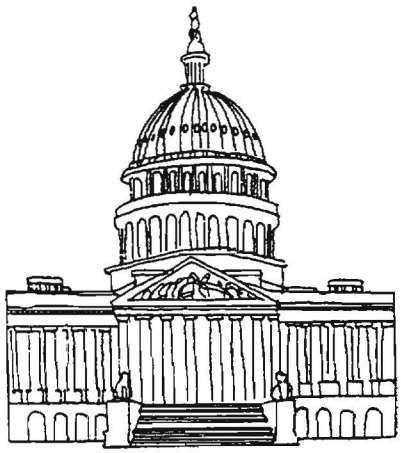
To submit articles and letters, please see last page

For New Subscription or Change of Address or Name

MAIL name and old and new organizations and building to:

Distribution, CRYPTOLOG, P0541, OPS-1
or
via PLATFORM: cryptlg @ curator *inoperative at*
via CLOVER: cryptlg @ bloomfield *present*

Please DO NOT PHONE about your subscription or matters pertaining to distribution



Address to the graduating class of CY-500, 21 May 1992 by the Honorable Helen Delich Bentley (R), Representative, Second District, Maryland

Good morning ladies and gentlemen and distinguished guests.

It is a pleasure to be asked to address you at a time like this in your lives, a time of satisfaction, a time of looking forward: graduation means not only an ending, but a beginning.

I do enjoy such an occasion, because in my own life, in my own experience, there have been so many endings to quite a few careers: reporter, editor, columnist, television producer and journalist, Agency chief, international trade consultant—all of the leave takings leading, eventually, to Congress.

It has been a demanding path, but rewarding and exciting.

And in Congress, at this particular time, I have to focus on the rewards of serving one's country in difficult times. The Congress, as a body, is struggling against a public perception of privilege and corruption and ineptitude.

To one identified with the Hill, it makes no difference that I bounced no checks (I didn't even have an account at the House bank), that I won a primary in March handily—with a fairly heavy turnout—that most of my mail is favorable, etc., does not affect the overall atmosphere. It is a very sad time for the establishment, and a very bad time for the country.

There is never a good time for both the Executive Branch and the Congress to be under siege from the press and the public, but in the political dynamic where timing is critical, conditions of the world demanding strong responses, strong support from the "leader of the free world", make a weakened Congress and a beleaguered President and the nation particularly vulnerable.

We face a $4 trillion debt ceiling this year, interest costs in excess of $1 billion per day, 12 to 14 million unemployed or underemployed, and a debilitated infrastructure: bridges, sewers, roads.

And a Europe in flux from the Volga through the Balkan Peninsula into the European Community: turning on itself, breaking off on all manner of trade agreements, threatening GATT, announcing the end of NATO with the establishment of a Franco-German corps.

The dissolution of the balance of power—some would call it a balance of terror—between the two super powers was anticipated, was discussed and written about, but there is no evidence from the behavior of this government ***that we were any more prepared to deal with it than were the Russians themselves***.

No aid package was in place that addressed the particular and peculiar needs of a fragmented USSR. The answer to the food shortages of the winter were massive shipment of grain, tried and

true business for the last twenty years for our commodities dealers—***when there was a stable government infrastructure in place to handle the movement and disbursement of commodities*** .

I led a drive in the Congress, with 119 congressional supporters, to have at least a part of the shipments be shelf-ready canned goods.

We, also, should have been ready to barter aid for influence in the decisions made on the sale of nuclear weapons. I should have considered: food or money in exchange for keeping weapons out of the hands of extremist groups.

Hard ball? You bet! Business as usual will not work when there is not one strong government to deal with, but a group of floundering governments driven by the need to survive.

This is true, also, on the Balkan Peninsula. It is not a situation that responds to the old diplomacy. The EC and the United Nations should be considering plebiscites called by constituencies ***which occupied territories in place prior to 1941***. Every effort must be made to reconstitute the nation of Yugoslavia prior to Tito's terrible policy of redistribution of minorities across ethnic territories.

Without proper planning, a reactive response frequently makes us a victim—as much as any of the participants—because without preparation, our responses are either inflammatory or inept. But once the house is really on fire—guess who is supposed to field a half million men and weaponry to put it out?

Iraq-Kuwait is a wonderful example of what we can do when the situation gets of of hand—however, along with such success goes a huge bill. But I hear little discussion about the U.S. policy prior to that time vis-a-vis Iraq and Kuwait. Had we been wiser, had we handled Iraq better, would we have had to be there in the first place?

Certainly the Panamanian action revisited tends to convince one that we were not well briefed on the local political scene, or if we were, we did not have a plan in place to respond to a popular uprising. Had we supported the domestic insurgency in the fall of the year, we would not have had to land our troops there in December.

Appropriate intelligence is of no value if it is not properly used. The horror of a modern war, comparable to the scale of WW II, is beyond the ability of the average American to imagine, and the costs beyond the ability of any nation to pay. We must short-circuit any of these threats by using intelligence—our brains—to counter modern force.

If it is true, as some believe, that the cost of ever-escalating weapons developments forced Russia into glasnost, it pushed us into bankruptcy.

Dr. Martin Van Crevald's book, *Transformation of War*, presents a strong case for the disappearance of "great wars" and the emergence of a series of low-intensity conflicts. Call them insurgencies or counter-insurgencies, label them riots in Los Angeles or revolts in Bangkok, civil wars in Yugoslavia—locale specific or country-contained, driven by local issue, no monolithic ideologies fueling the madness, the United States is placed in a leadership role, which demands policies based on regional histories, anthropology and sociology, and an acceptance of standards for the countries involved that are sometimes alien to the West.

It is long past the time that we can go into the world as soldier-preachers and receive any kind of welcome. If we would spread our values, it will be by example ***only.***

In order to do this well, timely information—all kinds of intelligence—about these countries will be of the greatest value. If Dr. Crevald's premise about the changing nature of warfare comes close to what is actually occurring, then the nature and focus of the intelligence community will have to change also.

The question becomes, then, who will initiate the changes? The National Security Act of 1992 (HR 4165) seemingly has received little support, inside or outside of the government. In a series of hearings held over this winter, the majority of the testimony from experts—former Agency officials and academia—seems to suggest that the legisla-

tion goes too far and may be seen as Congress trying to micro manage too much.

CIA chief Robert Gates testified, in answer to the proposed bill, on changes already under way in the structure of the Agency and in the efforts—across all intelligence-gathering departments of all agencies—to better integrate information and to share analytical findings.

It should be of special interest to you in NSA that when Director Gates was explaining some of the proposed changes in the area of strengthening the management direction and coordination of intelligence collection, he stated, "in making the structural changes that I am about to describe, I have used as a model some aspects of the National Security Agency, where one individual not only is able to task all of the signals intelligence collectors available to the DoD and the Intelligence Community, but also has the responsibility for establishing standards, ensuring interoperability and budgeting and strategic planning in this area."

He qualifies that position slightly by pointing out that "the collection disciplines are sufficiently different in that they all cannot, and perhaps should not, exactly be modeled on NSA. Indeed, none can." He continues by commending the basic idea of having one individual ultimately responsible for each discipline, with a specific responsibility for the coordination and management of requirements for that discipline, including oversight responsibility for standards and strategic planning.

Now, my mother always told me that imitation is the sincerest form of flattery. More than that, it tells me that the "NSA model" has proved itself over time, and that is worth much more than flattery.

Mr Gates' testimony on April 1st reported changes in focus in intelligence as early as 1980 when only 58% of the Community's resources were dedicated against the Soviet Union. By 1990 the figure had dropped to 50%. I am sure you are aware of this, but most of the Congress and certainly, most of the American people are not.

But of greater importance, to me and to the business community in this country, is the report from testimony by Mr. Gates on April 29th before the Judiciary Committee outlining some new thrusts for the remaining 50% of resources: tasking against foreign economic espionage.

Remember, the ultimate purpose of warfare is to seize the wealth of another country, to be able to use its resources, both human and material, for the enhancement of the aggressors' own nation. A successful leader achieves this at the least possible cost to his own people with the least damage to the territory taken.

Modern warfare cannot satisfy these demands any more. It is too destructive. It is too costly. Outside of the internecine wars, the popular uprisings, major nations in the 21st century will wage war with dollars instead of missiles.

I am heartened that Director Gates addressed the economic threat at such length. However, I am gravely concerned that neither the Congress nor the Administration has addressed changes in the legislation which recognizes this threat.

One particular area of concern to me: dual-use technology. There is a pattern, over my time in the Congress, of technology being bartered offshore: for foreign policy concerns, by the State Department; for economic concerns, the sale of T Bills and foreign investment, by the Treasury Department; for the profits of U. S. businesses, by the Commerce Department.

The only Agency with any concern for the long-term strategic position of the United States—DoD—frequently is outvoted by the big three. The actions of CIFIUS, a major case in point ***where not one sale of companies owning valuable state-of-the-art technology has been stopped*** by the Committee ***even when semi-conductor technology was involved.***

We are in a global economy, one into which it seems we slipped and slid, tumbled and fell ***without any preparation to protect the wealth of this great nation represented not only by its dollars and raw resources, but by its markets and its intellectual properties.***

Small U. S. companies are encouraged to go joint-venturing with foreign corporate giants, never understanding until much too late that a contract drafted under U. S. law is binding only so long as the small company has resources to stay in court for months, sometimes years enforcing the terms.

The IRS is running into the same court confrontations with these corporations that our small companies have faced. And, if you think that Uncle Sam has the deepest pockets and will win, consider this: currently there are 45,000 cases under dispute. Even the government doesn't have pockets that deep, and even though estimated underpayments run as high as $100 billion.

If I am frustrated that the great informational resources of this country are not being used to plan and prepare our policy makers well, how much more frustrated analysts must be. We work with statistics in our office, as broken out and basic as we can get.

Ladies and gentlemen, they are dreadful on the economy of the U. S.

They are frightening on the health of our people, both physical and mental. Recall when the intelligence community, using Russian data—I think it was in the '70's—came up with mass alcoholism as a major problem in Russia? The Russians promptly stopped printing the information.

Overlay those models on the U.S. Someone has been waging a very successful war against this country—devil, man, or nation, or a concordance of the three. We are in trouble, and as the President has said, you are the first line of defense.

Get the best information possible. Disseminate it throughout the government. Treat it honorably. We cannot heal ourselves if we do not know what is wrong—not only in the world, but inside our own system. Be courageous of the truth—there is no other way to secure freedom!

As Americans, we are the descendants of the toughest survivors of every nation on the face of the earth. We will endure.

I wish you well. God bless.

SUBSCRIPTION TO CRYPTOLOG

- ☐ Please enroll me as a new subscriber
- ☐ Please check my current mailing address
- ☐ Please change my mailing address
- ☐ Please change my name
- ☐ Please remove my name from the mailing list because I am
  - ☐ retiring or resigning
  - ☐ going to a field site
  - ☐ taking long-term training
  - ☐ too busy to read CRYPTOLOG (though I know I'm missing a lot)

OLD NAME AND ADDRESS		CURRENT OR NEW NAME OR ADDRESS	
Name (Last, first, mi)		*Name (Last, first, mi)*	
Org	*Bldg*	*Org*	*Bldg*

Mail to: Distribution, CRYPTOLOG
P0541 Ops-1

Over the years, I have often found myself extolling the value of publishing, pointing out to younger members of the workforce the value to the organization and to the individual of writing for publication. I do it for several reasons. First, I believe it contributes positively to the professional culture and climate of the organization; second, there seems to exist within NSA an unhealthy disinclination to publish, possibly due to a misreading or misunderstanding of our security rules and focus; and third and most important, because no one ever did it for me. I had to learn the secret for myself, and it took me the better part of my career, more than twenty years, to do so. Invariably, when I finish my little exposition, the employee tells me that no one in his or her entire career had ever pointed this out before and thanks me for doing so. It is as if I have let the person in on a secret of success that had hitherto been concealed.

Since at the rate I am going I will never reach more than several dozen of the agency's employees and since I now believe that there are literally thousands of others who might profit from my message, I decided to turn my little speech into an article so that more might be exposed to it.

It is hard to explain why publishing is not more aggressively pursued. I find it difficult to believe that the value in doing so has escaped everyone's notice. Security and the attendant shyness we have regarding undue public notice explains some of it, although there are numerous outlets for classified articles including our own *Cryptologic Quarterly* and CRYPTOLOG, there are many valuable lessons and insights from our work that can easily and adequately be dealt with in an entirely unclassified manner; and portions of the agency's work are unclassified anyway. Another reason, based upon the testimony of many employees, is that supervisors are not encouraging it — nor are they providing an example by publishing themselves. The sad result of this is a lost opportunity for the organization, the individual, and the profession. I would hope that some supervisors can be persuaded by this article. And finally, there is the matter of simple inertia. Publishing does require effort. But there is a payoff.

Having given the subject a fair amount of thought, I have come up with seven reasons why someone among the NSA workforce might wish to consider writing for publication.

Reason 1: It forces one to think more deeply about the subject.

We often think we understand a subject until we try to explain it to someone else or write about it. It is only then that we realize that we do not understand it nearly as well as we had thought. And so often, when we read something we have just finished writing, we are often embarrassed to discover that what we just produced simply does not hold together. This forces us to step back from the subject, think about it more deeply and work our way through the subject again. Oftentimes this even leads us to challenge some of our original assumptions and beliefs. The end result is that our understanding deepens. This is an extremely valuable process, the benefit of which accrues even if we never actually publish the article.

Reason 2: It can be an excellent source of psychic income.

No one should be embarrassed to admit enjoying being the beneficiary of a little psychic income now and then. Seeing in print something you have written is one of its best sources. Justifiable pride derives from the realization that someone else thought enough of what you had to say to publish it so that others could read it too. Actually, the psychic income can occur in two increments. The first increment occurs when you first see your piece in print. The second increment occurs when you discover that the published article has been cited by someone else. To have an article cited by another author has to be one of the highest forms of praise. I remember vividly the first time this happened to me. I was in a bookstore browsing when I noticed a book on a subject about which I had once written. I picked it up and was thumbing through it when I happened upon a footnote reference that began with my name. I promptly bought the book.

Reason 3: One can make money from it.

Under present law, even if you wrote an article entirely on your own time, you could not accept money for it. But you can enter it in some contest or other, and there are such contests all the time. Many of NSA's professional societies sponsor annual essay or writing contests with cash prizes. NSA's largest reward for writing, the Cryptologic Literature Award, carries a first prize of $2500, not an insignificant amount. One of CIA's publications, *Studies in Intelligence,* automatically enters any accepted article into an annual contest for the best article. The odds are quite good. There are four issues a year and approximately nine articles per issue. Last year, the publication awarded nine cash prizes. Thus, the odds of receiving a prize, once the article is accepted, is about one in four. And the prizes range from $200 to $2000.

Reason 4: A published work is an entry in a Personnel Summary or Resumé.

Resumés offer a chance to list your publications; NSA's own Personnel Summary has set aside a specific space for such a listing. It may be useful to know that there are some of us who always look specifically at the Publications entry to see what if anything is included. I realize there are not many people who do this, and therefore most would not notice if there were nothing listed. However, most of these same people would notice if something *were* listed. And certainly, any entry is better than a blank.

Reason 5: Publishing is a professional obligation.

Most people consider themselves professionals, though they may have done little to contribute to the advancement of their profession. It seems to me that if you wish to call yourself a professional, you should pay some dues to your profession. What you do on the job constitutes the dues you pay to that job; professional activities such as publishing constitute the dues you pay to your profession. Although there are many ways in which you can contribute to your profession, contributing to the literature of the profession is one of the best. Writing and publishing a professional paper confers upon the author considerable stature in the profession. Also, publishing is a professional activity with enormous leverage. Many people belonging to the profession can be stimulated by the article. What you write can inspire new thinking on the part of someone else. The reader then expands on your idea in another article. In this way, the profession advances.

Failure to publish is to miss this significant professional opportunity and, in my view, to ignore an important professional obligation.

Reason 6: A published work constitutes a part of your legacy

At some point in life, you realize that you are running out of time and you begin to think about what you will (or will not) leave behind. You begin to consider your contribution to the world, your legacy. Your legacy is what you pass on to future generations. It could take the form of material possessions, creative products, enterprises, or simply influence on others. Legacies are important. Ultimately, our legacy constitutes whatever claim we have on immortality.

Legacies are not generally a concern of the young. People tend not to think in these terms until they reach mid-life. I have noticed, for example, that people become more concerned with their legacies as the date of their retirement nears. This has certainly been true in my own case. In fact, it was probably an influencing factor in my decision to write this article.

I am sure that you have had the experience in which a valued, long-time employee finally hangs it up and retires. In the thirty-some years that one employee had worked, she had amassed a considerable amount of knowledge and experience. But because she had not written much of it down, when she retired, that knowledge and experience went with her. Now, several months later, the organization she left behind faces a thorny problem, its members note that if Thelma were still around she would know what to do. But of course, Thelma is not around, and neither is any reflection of her considerable experience. It is a sad situation: sad for the organization and even sadder for Thelma. Sad for her because there is a natural generative imperative in all of us to want to leave something behind. The Talmud contains the observation that there are three things one should do in the course of one's life: have a child, plant a tree, and write a book. All three are generative activities; all three involve leaving something behind that is likely to survive us; all three constitute part of our legacy. Publishing an article may be the first step to *your* book.

Reason 7: It makes it easier for your boss to get you promoted.

For those of you who have not been moved or influenced by any of the first six reasons, this seventh and last one may have some persuasive appeal.

I like to think of our promotion system as consisting of two gates. The first gate is a binary gate; it determines *whether* a person will or will not be promoted. This first gate is controlled by one's immediate supervisor and perhaps by the next person up. The second gate is an analog gate. It determines *when* the promotion will occur; and many, many people control this second gate, particularly for promotion to the higher grades.

A key group of people who exert influence on the second gate are promotion boards. Among other evidence, promotion boards receive written and oral testimony. Because they read and hear so much testimony, most of it glowing, they become anesthetized to adjectives. It would take a very creative testifier to come up with an adjective that a promotion board had not heard. Every person that the board is considering is hard working, highly motivated, tenacious, highly effective, etc. If it were were not so, that person would not have been recommended for promotion in the first place. Nevertheless, the testifier has to offer up a suitable serving of adjectives just to keep that candidate even with the others.

The testifier is then likely to relate some recent contribution that the candidate made that is considered particularly significant. The problem is that there is a strong likelihood that most of the board members will not understand nor appreciate the significance, because the contribution is in a field or discipline foreign to theirs. Nevertheless, the contribution is presented. To the typical member of the promotion board, the contribution certainly sounds positive. Clearly having made the contribution is better than not having made it. But how does it compare with the specific contribution of another candidate in an entirely different field, both of which are foreign to the direct experience of the board member? How is the board member supposed to compare the contri-

bution of a mathematician with that of a lawyer, or a linguist, or a logistician? Yet that is exactly what members of promotion boards are required to do. Again, the testifier has to present such a contribution, but because of the difficulty in comparing them, the net effect may be no more than to keep her candidate even with the competition.

If, however, the testifier is then able to produce some published work of the candidate, that candidate is likely to slip ahead of the others. Why? Well, first of all because most of the competition will not have anything published. Second, and perhaps more important, all members of the promotion board can identify with a published work. They may not understand what was written (they won't take the time to read it anyway) but they know what it means to publish. They all know what it means to write and they all know what it means to have one's work deemed worthy by some outside arbiter and actually published. Having done a bit of testifying before promotion boards myself, I can attest to the utility of this strategy. I have used it successfully on several occasions.

So there you have it: seven good reasons to write for publication. I hope I have stimulated you to consider doing so. I look forward to seeing some of your names as authors of future articles.

The Lead Sentence in a Serialized Report

SIREN
SIGINT REPORTERS NOTES

P.L. 86-36

[redacted] P05211

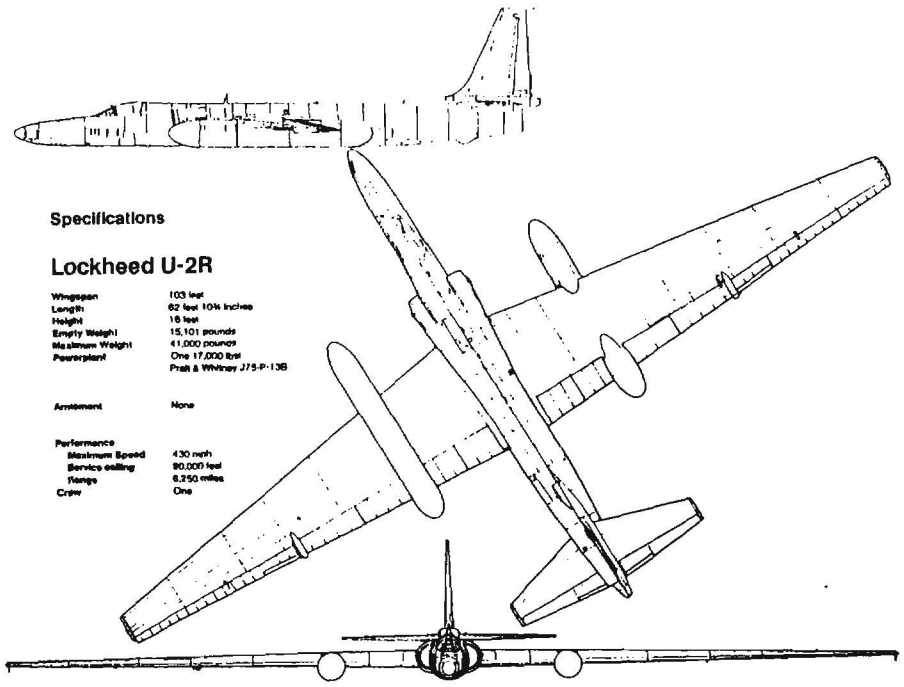
The lead or topic sentence of a well-written SIGINT report should concisely convey the essential facts of the report to provide the reader, especially the time-pressed executive reader, with a well focused précis of the contents of the report. This lead sentence should always answer, when possible, the "Five W" questions —who, what, where, when, and why. It should expand upon the title, focus on the main theme of the report, and highlight the most significant foreign intelligence and any conclusions drawn from the SIGINT facts. Reporting the "who" is vital to the SIGINT user for assessing the importance of the information.

While the lead sentence should expand upon the report title, it should not be cluttered with clarifying data such as unit subordinations, coordinates, abbreviations; such information should follow later in the report. In a short report, this information would be in the second sentence or paragraph, and in a long report, in the section labeled "DETAILS." Note that short reports do not require sections headings, but long reports require at least the sections heading labeled "SUMMARY" and "DETAILS."

Elaborations of this guidance are contained in USSID 300, Sections 4.3 and 6.2.

[redacted]

P.L. 86-36



UNCLASSIFIED

Figure 2. Lockheed U-2R

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

~~(C)~~ Remote airborne operations have long been a major part of this country's overall SIGINT effort. Over the years, we have employed several types of airborne platforms and have enjoyed excellent success in accomplishing our mission. However, these conventional platforms have limitations that somewhat restrict our collection potential. This article will show the support to military operations provided by the [redacted] through its involvement with the highly capable U-2R aircraft.

HISTORY

(U) The history of the U-2 is unique. Developed in the early 1950s by Lockheed, the prototype resembled a jet-powered sailplane with a slender fuselage. It was 49 feet 8 inches long with a wingspan of 80 feet 2 inches. To balance the wings, a set of dropable stanchions with small dolly wheels (called pogos) were attached at mid-span on each wing. These fell away when the aircraft took off and were retrieved by ground crews to be reused when the aircraft landed.

~~(C-CCO)~~ By the late 1960s the aircraft had undergone dramatic changes. The new U-2R's (R for revised) overall length was increased to 62.7 feet, with a wingspan of 103 feet and a range of 6200 miles. However, the true utility of the U-2R was seen in its ability to operate at altitudes in excess of 60,000 feet. This capability benefited SIGINT operations by making platform detection and interception more difficult and by allowing a deeper look into the target area than afforded by conventional airborne efforts.

[redacted]

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

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

REFERENCES

(U) Larry Davis, *U-2 Spyplane in Action*, Texas, Squadron/Signal Publications, Inc, 1988

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

Stuart Buck, ret.

The Accidental Lexicographer

(U) Fifty years ago we were in the darkest days of World War II. Experienced linguists were urgently needed for translating and for code and cipher work. Stu Buck was among the seasoned scholars of language called to the colors.

~~(S-CCO)~~ Operationally he worked on Japanese, Chinese, Romanian, French, Mongolian, Tibetan and Dzongkha as a bookbreaker and cryptolinguist, as well as a lexicographer.

(U) This article is based on a talk to the Crypto-Linguistic Association at an unknown time.

~~(FOUO)~~ Sometimes I think that I have been involved in lexicography, to a greater or lesser degree, throughout my entire career at NSA. The projects have ranged from small informal card files stashed away in my desk to a regular, full-fledged dictionary. For our discussion today, I shall confine my remarks to three dictionary projects, each of which had certain distinctive features.

The Japanese Technical Dictionary

~~(S-CCO)~~ At the end of World War II, I was asked to assist in compiling a Japanese technical dictionary. Certain aspects of this particular project were unique in my experience. First of all, the task itself was taken seriously. No one viewed it as busy work. Linguists were carefully selected for their special skills—and tested in order to determine that these skills were not illusory. Once the group was set up, it stayed together until the project was completed. Guidelines were made crystal clear to all involved—and were enforced. It was all very simple: we were told to extract from various dictionaries any technical terms not included in *Kenkyusha*, the standard dictionary.

~~(S-CCO)~~ I was assigned to work on a French-Japanese dictionary, so my basic task was to translate the French expression and to determine, as best I could, if the Japanese equivalent was acceptable. All my cards were checked by another French linguist; then we turned them over to [redacted] the editor-in-chief—and a superlative Japanese linguist. P.L. 86-36

~~(S-CCO)~~ We saw the trees, he viewed the forest, and took personal responsibility for the overall product. I recall that there were about a dozen linguists in our group, working from lists of Japanese words defined in some other language—or, in a few instances, from Japanese sources. Streams of cards flowed to [redacted] who accepted or rejected items in terms of his basic objectives. The high value of the dictionary that was finally published is suggested by the fact that the publishers of *Kenkyusha* appear to have incorporated it intact into their latest edition. P.L. 86-36

(U) I soon found myself writing essays on all the key words encountered, including as many example of usage as I could find. I had little choice but to use the eclectic method, so I examined, for every word under study, everything said in every available dictionary, compared the results, added what I had gained from my own experience, and made out a card for my files.

P.L. 86-36

(U) The whole thing was totally foolhardy. In a sense was trying to do all alone what had been accomplished by [redacted] highly trained team.

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

~~(C-CCO)~~ Give me credit, however. I realized that it was madness, but I never took my eye off that [redacted] Thus, I tended to go easy on the flora and fauna, and to bear down heavily on common vocabulary, particles, function words, idioms, likely loan words, personal names, titles, place names, organizational terms, hierarchies of all types, etc. Until the very end, I viewed the dictionary as a technical aid required to solve a specific [redacted] problem. Perhaps I went overboard, but it seemed to me that the problem demanded quite a lot. Even so, I was surprised to discover that the dictionary, when completed, contained some 833 pages.

[redacted]

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

[redacted]

(U) Included in the listings were a gazeteer and a list of personal names. There were three sorts:

- transliterated Dzongkha, in true dictionary order;
- a phonetic transcription, according to a system devised by Indian scholars; and
- English meanings.

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

(U) I like the system of deriving vocabulary from current texts and the ability to correct, update and edit periodically, but I miss the essays or articles that were characteristic of key words in my Tibetan dictionary.

Problems in Lexicography

(U) Certain problems were common to all three dictionary projects described above. Most important of these was the answer to the question, "what shall I include, and what shall I leave out?" Exactly what am I trying to do: tend a dustbin or forge a precision tool?

(U) Also, who will answer for the final product, a lot of anonymous contributors or a single individual? What shall I do about things I do not understand—ignore them and hope they will go away? Suppose I understand some tricky expression or usage that is devilishly hard to explain to someone else? Can I assume that everyone else understands it just as well, and save myself the trouble of clarifying it?

(U) Is it enough to provide one-for-one equivalents (if there is such a thing), or am I, as lexicographer, obliged to get into language structure?

□

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

~~(C-CCO)~~ Once upon a time there were graphic linguists and voice linguists, and then there were cryppies. At that time and place I was called a "cryppie." Not a cryptanalyst, mind you, but a language person

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

~~(C-CCO)~~ A good command of the language was and is absolutely essential for this work.

~~(C-CCO)~~ Well, since I did no reporting, and translated only an occasional cryptanalysis-related message, I didn't feel like a graphic linguist, and so I started thinking of myself as a cryptolinguist. (Perhaps this was in self-defense, as linguists would always see me as a "cryppie," while cryptanalytst would refer to me as a "linggie.")

~~(C-CCO)~~ But once in Z, I discovered that there was a whole other world out there. While in some languages cryptolinguists need a great degree of depth—years of experience, target knowledge, and excellent language skills—other Z people worked on targets which required somewhat less depth but more breadth—introductory course in language, possibly in a number of languages, but requiring far more knowledge of cryptanalytic techniques.

~~(S-CCO)~~ So what is the correct definition of the term "cryptolinguist?" The Glossary of Cryptanalytic Terminology (30 Sept 91) defines cryptolinguistics as "the branch of study embracing the characteristics of language which have some particular application in cryptology

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

[redacted]

(C-CCO) The question remains, "What is a cryptolinguist?" And, "Am I one?"

(C-CCO) Over the years, many people have met for countless hours to try to put together a COSC for cryptolinguists. Yet the toughest part of that is defining what a cryptolinguist is. Is this a broad field encompassing both those "majoring" in CA but using language daily, as well as those who "major" in language [redacted] How do you set up criteria for a COSC that covers both? Must a cryptolingist be professionalized in both fields?

(C-CCO) Or are these really two totally separate fields? It has been suggested that the cryptanalyst using language is a cryptanalyst, and should be considered as such by tech track boards, etc. But what of the language-cryptolinguists?" Are they cryptanalytic enough to be considered (fairly) by CA boards, or must they earn their accolades elsewhere—through A and B Group language boards?

(C-CCO) If we define a cryptolinguist as someone who is somewhere on a continuum that stretches between two poles, language and cryptanalysis, but who needs to use both, we could embrace both the language-cryptolinguist (needing depth) and the cryptanalyst who uses language (needing breadth). A COSC could be set up with two tracks, the primarily CA track, and the primarily language track, working with both the CA and Language career panels.

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

(S-CCO) [redacted]

How will they be treated by language boards? Is as much value given to cryptolinguists as it is to voice linguists? (For a clue, look at FLIP allocations.) If we had not been split up, would there be enough of us to consider as a separate group?

(C-CCO) What do you think, linguists, cryptolinguists, and cryptanalysts out there? Is there any chance that we can finally come to a consensus on what a cryptolinguist is? Can we come up with a COSC which encompasses both those strong in language and those strong in cryptanalysis? Or should these two groups of people be treated separately?

(FOUO) I would like to hear your views. You may call me on 963-5071. On e-mail I can be reached [redacted] or hard copy can be mailed to me at Z443, Ops-1. Your responses would be most welcome.

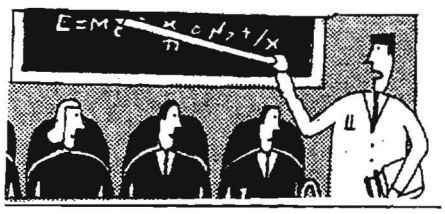
P.L. 86-36

Answers to Electronic Publishing Quiz, page 36

1. Advanced Function Printing
2. All-Points Addressable
3. Computer-aided Acquisition and Logistics Support
4. Cathode Ray Tube
5. Dynamic Job Descriptor Entry
6. Dots per inch
7. Disk Operating System
8. Forms Description Language
9. Generalized Markup Language
10. Job Control Language
11. Job Entry Subsystem
12. Magnetic Ink Character Recognition
13. Optical Character Recognition
14. Overlay Generation Language
15. Print Description Language
16. Print Service Facility
17. Revisable Format Text
18. Standard Generalized Markup Language
19. What You See Is What You Get
20. Xerox Escape Sequences

Major Breakthrough in Combinatorial Mathematics

[redacted] R51



A major breakthrough in combinatorial mathematics has been achieved in R51, where researchers constructed a ***Hadamard difference set in a group of order 100***—a feat thought to be impossible by most experts in design theory, a highly developed science in which conventional wisdom held that the order of such a group could not have a prime factor greater than 3.

The new difference sets provide a means of constructing highly structured block designs and related Hadamard matrices which are square arrays with entries +1 and -1 and whose rows are pairwise orthogonal. Such arrays have a myriad of applications in areas as diverse as statistical design and coding theory which exploit their pseudorandom correlation properties. These properties are similar to those of M-sequences, bent functions and perfect binary arrays which correspond to difference sets in more familiar *abelian* groups.

Until this recent discovery, the only known Hadamard groups had order of the form $4N^2$, where $N=2^a3^b$. Since the family of Hadamard groups is closed under products, the new result may be combined with the old to produce Hadamard groups of orders of the form $4N^2$, where $N=2^{s5^{s+1}}$ or $N=2^a3^b10^c$. There is hope that these constructions may be generalized to produce Hadamard groups of any order $4N^2$, $N=2^a3^b5^c$, and perhaps others as well.

The new result also provides a counterexample to a long-standing conjecture of Thomas Storer of the University of Michigan that a nontrivial difference set could exist in a nonabelian group only if there exists a difference set of the same size in an abelian group of the same order. It is ironic that the nonexistence of *abelian* Hadamard groups of order 100 was proven recently by University of Minnesota-Duluth researcher R. L. McFarland who was the one who promoted the subject of difference sets in the Agency when he was stationed here as a young Air Force lieutenant twenty-five years ago.

The break-through work was performed as part of a project to determine which (if any) of the sixteen groups of order 100 could contain a difference set. The four abelian groups were ruled out by McFarland, and, of the twelve nonabelian groups, six had been ruled out by the combined efforts of R. [redacted] R. L. McFarland, [redacted] Work was then focused on the six remaining undecided groups, and in particular, on the so-called G_9. P.L. 86-36

Ken Smith of Central Michigan University, here on sabbatical last year, outlined an approach to this problem and did a preliminary computer search which reduced the size of the final search (the sought-after difference set is a 45-element subset of the group of 100 elements, but trying all such subsets is out of the question). [redacted] did a more careful costing of algorithms to effect the final search and did more computing to build a database which would constitute the search space for a branching algorithm. In early January the approach looked feasible but had not been programmed. [redacted] presented a status report on the project at the Baltimore meeting, expressing optimism at the prospects of G_9. Other duties then intervened.

In anticipation of the AMS meeting at Lehigh 11-14 April [redacted] resurrected his work and enlisted [redacted] to write the final program. Ted quickly wrote a very clever C-program which effectively found all difference sets in G_9, and thus, immortality. ▫

Strategic Considerations for NSA Processing

~~(C)~~ The purpose of this article is to evaluate the likely effect upon NSA processing of technological and non-technological factors over the next decade and to propose strategic considerations for evaluation in determining how best to deal with these changes. In particular, this document seeks to update the prior Future SIGINT Capabilities (FSCS) documents with respect to NSA processing.

~~(C)~~ The User Interface System(UIS) is a multi-level ADP architecture that is intended to satisfy current and projected analytic support requirements, while providing an individual user with access to data and services regardless of physical location. It represents a long-term continuing effort, already well underway, to specify and provide an architecture that adapts to changing and evolving processing and support requirements. As such, it becomes the starting point for the strategic considerations developed in this document. The basic UIS (3-Tier) architecture is illustrated in Figure 1.

THE DISTRIBUTION OF PROCESSING

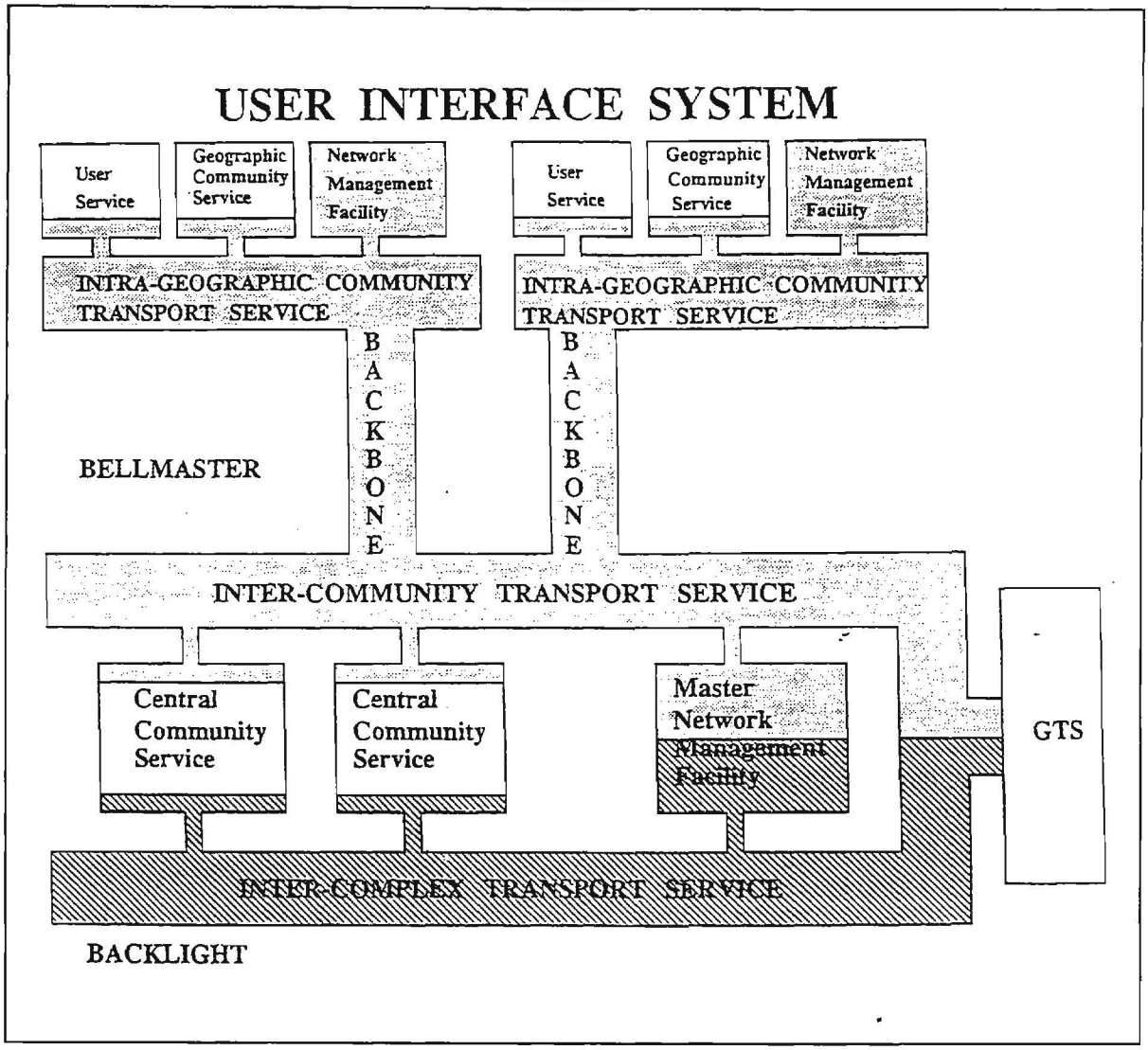
3-Tier UIS Architecture

(U) The high-level UIS architecture (Figure 1) developed in the early 1980's was predicated upon processing trends at that time, and mirrored industry expectations and architectural trends of that period: widespread processing distribution with decrease of large mainframe processors. Users were expected to interact, through either "smart" or "dumb" terminals (Tier 1), principally with intermediate (often referred to as "departmental") capability computers (Tier 2), where the bulk of the processing needs for that community of users was expected to be accomplished. These Tier 2 processors (typically thought of in terms of the mini-computers of the day) would, where necessary, communicate with a relatively small number of increasingly powerful mainframe computers or computer complexes (Tier 3) for compute-intensive ("number-crunching") processes; for access to (and often down-loading of) portions of very large data bases; and for eventual storing of processed data which might be needed by users outside the immediate community. Users were expected to have little concern with the mainframes which might be accessed, since the primary processing would be accomplished by the ever-more-numerous Tier 2 computers.

(U) The 3-Tier architecture is currently the accepted standard for a large installation—and is pertinent to smaller installations as well, principally by eliminating the need for one or more tiers—and is expected to be relevant well into the next century. The basis for the Tier definitions has already changed, however, and will change further as technology evolves.

Processing Distribution Trends Among Tiers

(U) Already the "personal computer revolution" has exerted great influence. There are very few "dumb" terminals still in use, and even "smart" terminals have been largely supplanted by powerful personal workstations. As the power of these workstations increases—already the high-end Tier



1 processors are approaching the power of the early supercomputers—more and more processing will be, and is, accomplished in user areas. This capacity and the increased sophistication of end-users are certain to support the momentum toward dispersing processing functions to Tier 1. It is likely that in a few years, most tasks previously carried out in Tier 2, and many in Tier 3, will be accomplished routinely in Tier 1.

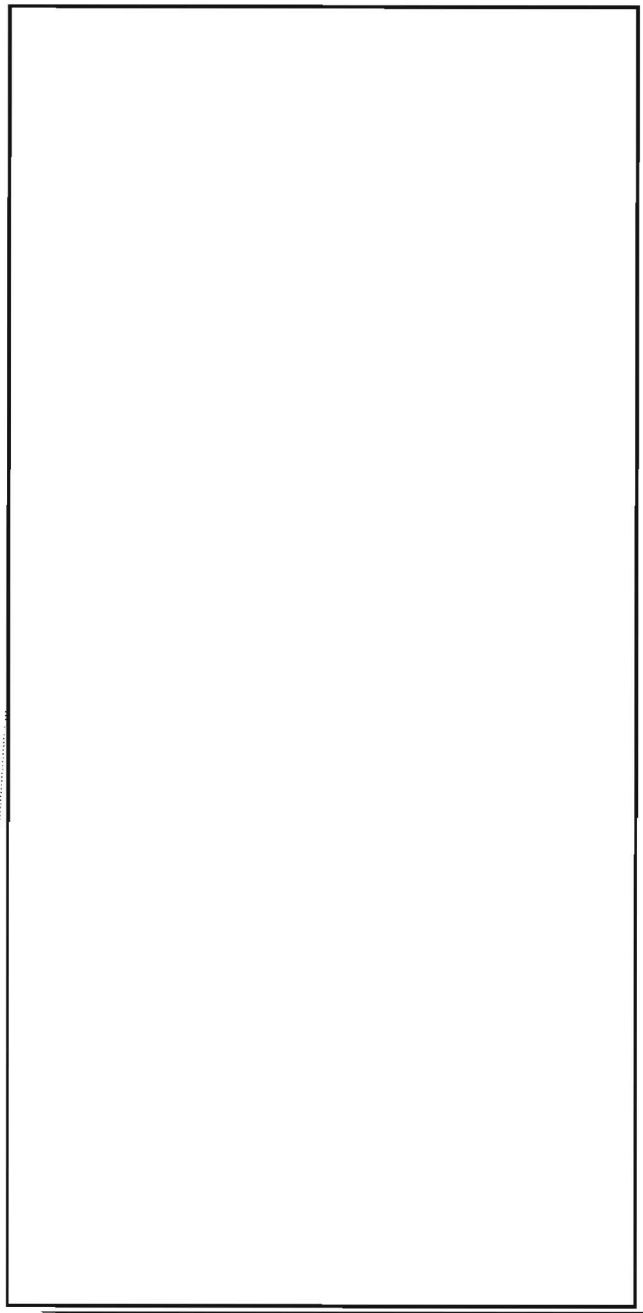
~~(C)~~ That leaves a less predictable future for Tiers 2 and 3. Some need for Tier 3 processing appears to be certain for the foreseeable future, at least for certain highly computation-intensive processes such as cryptanalysis, and for storage and retrieval of very large databases, only a small subset of which might be relevant to any particular set of users. It is possible, however, that the majority of the functions now carried out by mainframe complexes might migrate to the next (substantially more powerful) generation of Tier 2 (departmental) computers, serving to replace those current Tier 2 processes which will migrate to Tier 1.

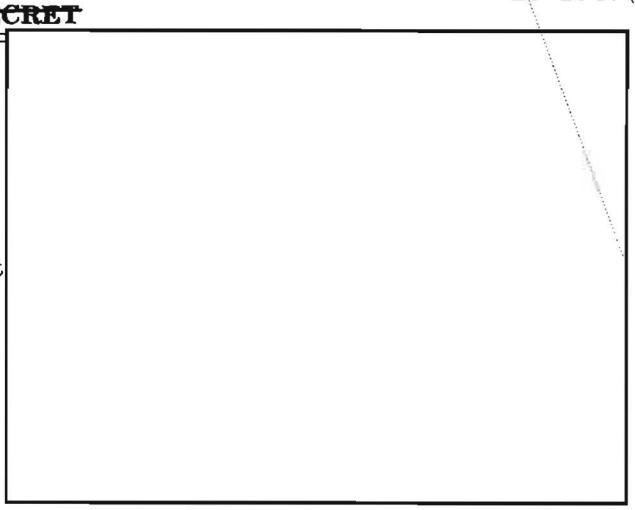
(U) Another possible scenario, which appears to be somewhat more likely, is that most of today's Tier 3 processing will remain in Tier 3, whose computers will also become ever-increasingly more powerful. If this happens, it is likely that much of the Tier 2 processing that is not suitable for Tier 1 may be redistributed to Tier 3, leaving the very real possibility that Tier 2 will largely disappear. There is much in favor of such a coalescence, including architectural simplification, reduction of support costs, reduction of operator costs, and simplified network management. Opposing this are the cost of mainframe processors, vendor flexibility, power and air conditioning needs, and,

possibly, elimination of whatever security benefits may be inherent in the use of departmental machines. Both industry direction and cost-benefit analysis will influence the choice.

(U) It is safe to say, however, that Tier 2 will remain relevant at least into the late 1990's, albeit with a reduced and less important role, such as support for Tier 1, rather than processing functions per se. Likely functions include those of file servers, traffic distribution, database repositories, and input/output support processors for Tier 3 processors.

The Distribution of Processing





MAN-MACHINE INTERFACE

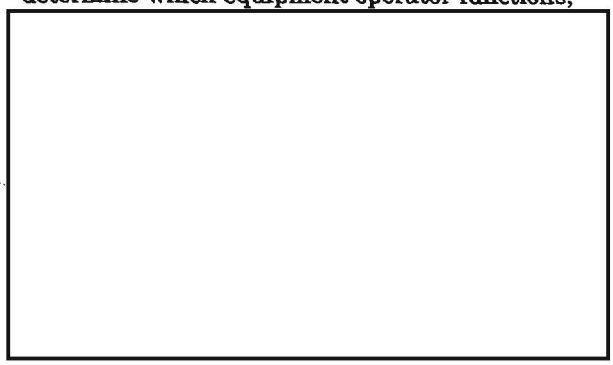
Standard User Interface

(U) There has been much discussion, both at NSA and elsewhere, about the desirability of having a single, user-friendly mechanism to permit any class of operator to interface with the equipment. An early goal was to define and implement a standard interface for all programmers, operators, and analysts who deal with computers. At first it appeared possible to come close to this goal in terms of a single workstation (ASTW) with a single keyboard configuration, connected to a single intermediate computer (ASH), using a single operating system (UNIX), and a single programming language (C). Now we know that none of these assumptions has, or will come to pass. We realize it to be a nice theory with more apparent than real benefits and at a staggering cost, if in fact it proved to be technically feasible. It did not address the problems of freezing on outdated technology in a rapidly changing field.

Realizable Man-Machine Improvements

~~(C)~~ The planned use of windowing software packages for high performance workstations permits access to many systems through a single keyboard and workstation. This in itself is a major improvement in man-machine interface, simply by requiring an analyst or programmer to learn only one machine, keyboard, and set of procedures for any given job. Now that the basic technology is here, there is a need to acquire modern workstations with state-of-the-art user interface devices and capabilities, and to train our workforce to make use of them. Further analysis is required also to

determine which equipment operator functions,



P.L. 86-36

STANDARDS AND PROTOCOLS

(U) The use of standards, particularly standard protocol suites, is required by the UIS architecture and is essential for achieving interoperability and commonality among differing functions and systems. Even though the Agency is in the process of adopting a much more flexible hardware standards program, its principal standards efforts are moving away from the low-level standardization on hardware and toward the higher-level standards available for both software and protocols.

Problems

(U) Since the mid-1970's, there have been increasing Agency efforts to provide a degree of standardization on computer hardware in an attempt to curtail the enormous support burden inherent in a multi-vendor, multi-component environment, and also to try to achieve the obvious benefits of system compatibility by use of identical hardware. As the computer marketplace has evolved toward the widespread use of standardized packages of both hardware and software, the Agency has attempted to do the same. It has become obvious, however, that a single choice for any given purpose cannot handle the multiplicity of uses which Agency elements require. As a result, standardization efforts are moving increasingly into the realm of software and, especially, protocol standardization.

(U) The focus of NSA's software acquisitions has clearly swung toward UNIX-based systems. This trend can be expected to continue and it is expected to enhance software portability and to make commonality among different NSA systems easier to achieve. Nonetheless, it is not a panacea. In particular, there is as yet no "standard UNIX" nor is there likely to be one in the near term. Moreover, as hardware becomes relatively cheaper with respect to total system cost, system vendors increasingly differentiate their products with "value added" software functionality. As a result, the software features available from vendors are not common across the industry and will not be so in the future. If one NSA element makes heavy use of proprietary "value added" features of one vendor or consortium of vendors, portability to a different element or application may be lost.

(U) Although software or hardware standardization may alleviate some difficulties that hinder interoperability, it is difficult to achieve commonality, let alone standardization, for many reasons. While commonality is a rational goal (to promote software cost sharing, for example), the real key to SIGINT production in a joint environment is system interoperability. System interoperability can come about most easily when the parties involved are following the same architecture, which is heavily dependent upon common usage of a set of standard protocols at all logical levels. Unfortunately, although NSA and other organizations are moving in this direction, there is not yet widespread availability of stable commercial packages that implement the protocols necessary at all levels. It is reasonable, however, to expect this problem to be resolved over the next few years.

Movement Toward Standards

(U) It has been the case, and will continue to be, that there exists a multiplicity of available standards in any given arena. In most cases a choice from among a (hopefully) small set of "acceptable standards" will be available to implementers. Even in cases in which we attempt to use a single standard, the magnitude of the installed base together with the rapidity of technological (and standards) change make it unlikely that we will ever deal exclusively with a single standard throughout the processing system. There must, however, be an increasingly strong movement away from vendor-proprietary technology and toward the use of open standards and components which can be acquired from multiple vendors.

Even here it is unlikely that large segments of the installed base will actually be converted, largely because of the immense investment in software. Rather, we must attempt to encapsulate proprietary communities, minimize the proliferation of proprietary technology to new systems, and provide "standard" gateways and bridges to interconnect the proprietary complexes to the external, open UIS world.

Categories of Standard

(U) Regardless of the type of standard, experience has shown that a single, usable-in-all-situations standard is probably neither achievable nor desirable. Rather, small families of "acceptable" standards should be defined in most instances, to balance the conflicting needs of interoperability and lowered support costs with flexibility of choice and optimization for a given environment. This leads to a grouping of standards in three basic categories:

(U) ***Mandatory Standards*** These are, and must remain, few and far between. Currently there is a single mandatory standard for the USSS, that of the network address protocol standard, currently the DoD Internet Protocol "IP." This is necessary in order that all systems throughout the SIGINT system can address one another and mutually interact, but even this requirement is less than absolute. IP must be made available for exchanges between communities, but it is not mandated for use within a local community of users. Moreover, some complexes, historically dependent upon a given vendor and that vendor's proprietary protocols, are unlikely to provide even IP as a canonical in the foreseeable future, relying instead upon their own internal protocols and on gateways to make the necessary translations to the standard world outside.

(U) ***Recommended Standards.*** In addition to "required" standards, there will be an increasing number of "standards of choice," recommended for use unless there is strong rationale for using a competing standard. Reasons for such recommendations may include both technical and resource-oriented rationale, to include economies of scale, bulk-buy discounts, user familiarity, and ease of portability.

(U) Thus the UNIX operating system is highly recommended for most applications (and will be even more so as the various versions of UNIX coalesce toward a single universally recognized standard). There may always be some applications for which UNIX is inappropriate and some (especially large mainframe-oriented) complexes for which its introduction within a reasonable period does not appear to be feasible (technically or economically). Still other areas may have an installed software base, dependent upon a competing operating system, which may preclude any movement toward UNIX.

(U) Similarly, a relational DBMS is recommended for most applications, with the highly available and economically competitive INGRES recommended as the DBMS of choice. However, it is recognized that there are some applications for which this choice would be inappropriate, and for which a different relational DBMS or a traditional hierarchical inverted file DBMS would be more sensible. Such choices should not be dictated, and system designers should be free to choose an alternative for cause. In the same vein, certain DoD standard protocols (e.g. TCP, the transport layer networking protocol) may be recommended as the protocol of choice for most applications. It is recognized, however, that the associated capabilities (and, often, overhead) may not be justifiable for some applications, and also that emerging competing (e.g. Open Systems Interconnect) protocols may be an appropriate alternative even in advance of acceptance of the full OSI protocol suite.

(U) ***Selectable Standards.*** There will continue to be many instances in which selection from a small set of approved standards will be acceptable, permitting system designers the flexibility necessary to make an informed choice for a particular application, while still adhering to the requirements for meshing with a controllable, supportable architecture. For example, one can select freely from among the various higher-level standard DoD protocols, and this freedom of choice will undoubtedly continue after OSI is embraced.

(U) With respect to languages, we will attempt to reduce the number which are used (and thus must

be supported), but will not try to impose a single language for all purposes. It is likely that use of "C" will continue to increase within the class of applications for which it is appropriate; FORTRAN use, though likely to fall off, will not disappear in the near future; and use of Ada will increase, especially for new applications, eventually supplanting many of the older languages such as PL/I. For networking, IEEE 802.3 (Ethernet) technology is expected to predominate in the near future, yet IEEE 802.5 (Token Ring) will likely increase within its own realm of applicability. By the mid-1990's, FDDI (Fiber Distributed Data Interface) is expected to be the dominant technology.

(U) Regardless, existing proprietary technologies will continue for the foreseeable future within existing local complexes, due to their widespread use in many of our current applications. They will, however, become increasingly encapsulated within the complexes where they predominate, and standard, commercially available interfaces will be used to connect them with other elements of the processing system. Their use will gradually wither and die out, as they are replaced by new or updated systems in which standard, open protocols are built in.

Summary

(U) The use of standards, of all varieties, is key to our architectural planning and is essential to meet our requirements within acceptable cost. However, standards should never be viewed as absolutes, and must be used in a sensible rather than dictatorial manner. In particular, practicalities indicate that the most promising road to compatibility and easy accommodation of technological change is by emphasizing well-defined protocol and interface standards which are widely supported and available. Secondary benefits will result from use of common software to the extent possible. Standardization of hardware, while very beneficial in areas where it can be accomplished, is very difficult in a broad sense. It is incumbent upon system designers to be aware of the various standards available, to consider carefully the benefits which they offer, then to make a reasoned decision, accepting in advance the problems which will arise if they select a different choice for cause.

CONNECTIVITY

UIS Connectivity Goals

(U) The requirement to provide connectivity among the various systems and personnel within the USSS is the most basic goal of the User Interface System architecture. The strategy for achieving this is, once again, to follow the lead of industry wherever possible and to concentrate on use of commercially available components and standard protocols. Our connectivity requirements are very similar in concept to those faced by a broad array of industrial and governmental organizations, although the number of connections, anticipated data volumes, and geographic dispersity of our environment present particular problems faced by only a few. Three UIS connectivity precepts affect all network planning:

All-to-All But Not Any-to-Any

(U) To meet the basic UIS goal of providing any user, at any location, with whatever processing and data resources are necessary to accomplish its job, it is necessary to provide the technical capability for any person or system to interconnect with any other person or system. At the same time, it is necessary to provide the capability to restrict such paths to those that are permitted and necessary for operational and security reasons.

Networks Must Accommodate Devices

The USSS processing system does, and will, encompass a vast array of systems and devices, from many vendors, representing a variety of technologies and technical generations. It would be unreasonable and unrealizable to require each potential vendor to make special modifications to its standard product line to interface to our networking structure. As a consequence, our networks must be designed to accept, unmodified, connection of this array of devices. This requires, once again, use of standard network technologies, standard protocols, and standard interfaces, all compatible with the technologies and protocols supplied as a matter of course by the majority of systems being produced by the various vendors

Management and Security

(U) Although network management and security are problems faced by all large organizations, our needs are, and will remain, more severe and more stringent due to the size and diversity of our system and, especially, to the unique security requirements which we must meet. It is in this area, probably more than any other, in which we will have to push industry to meet our needs, fund special developments, and utilize much in-house expertise to satisfy our requirements

Network Segments and Technologies

(U) Global networking in the 1990's and beyond can be thought of as consisting of five categories of networking segments (four UIS, one GTS), each with different requirements and each, at least potentially, using a different type of technology. These segments are the following:

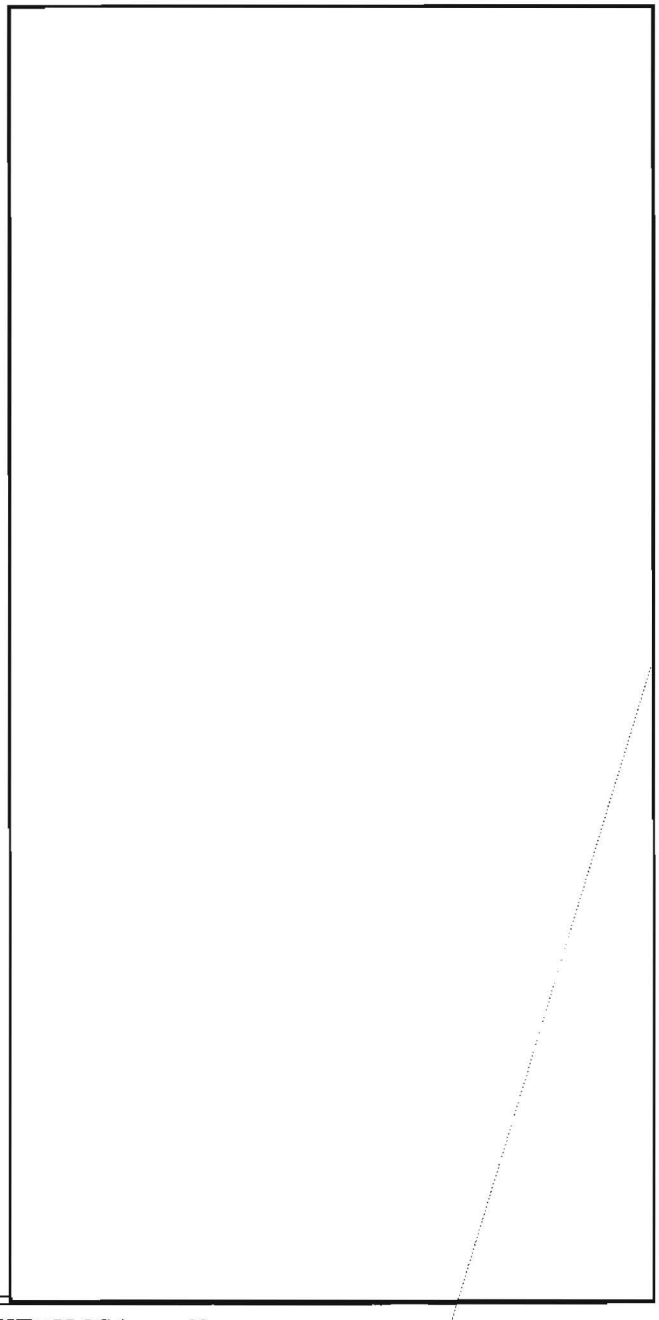
User Area Local Area Networks

(U) These LANs will interconnect user workstations and small departmental computers or servers within a local area, often defined in terms of a community of interest. Typically these are 10 Mbps ETHERNET (IEEE 802.3) LANs today, and this technology is expected to dominate in the near-to-medium term. By the mid-1990's we will likely still have ETHERNETs in place, but 100 Mbps FDDI fiber optic LANs will become dominant, as fiber is extended into user areas throughout the system. This technology should remain adequate for such use well into the following decade, and cost considerations indicate its early replacement to be unlikely.

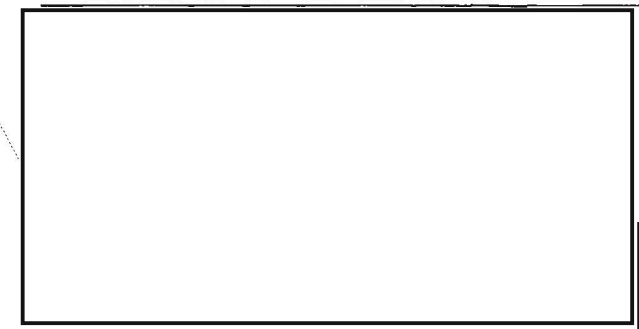
Interactive Backbone Segments.

(U) These high-speed LANs are used to interconnect user area LANs with one another, with intermediate (i.e. Tier two) processors, and with central processing complexes. BELLMASTER 1.5 (80 Mbps) backbones are being installed to satisfy this requirement today (under Project CLOVER), and BELLMASTER is expected to become the ubiquitous controllable, supportable architecture. For example, one can select freely from among the various higher level standard DoD protocols, and this freedom of choice will undoubtedly continue after OSI is within NSAW in the very near future, and ultimately throughout the system. This technology will be upgraded to FDDI as soon as it is available, and might well be upgraded again to enhanced FDDI (probably 200 Mbps) during the course of this decade, assuming that this technology is defined and becomes available. Even the basic FDDI version should remain adequate into the next century, however, and a replacement of markedly different technology is unlikely, principally for cost reasons. This technology can be expected to be standard, consistent, and long-lived throughout the system.

Inter-Complex Segments



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



Wide Area Network (WAN) Segments

~~(C)~~ The final category of segment is the WAN, which will be defined under auspices of the Global Telecommunication System (GTS). These segments will be used to interconnect instances of UIS (i.e. campus processing complexes) at each facility throughout the world. Represented by a variety of communication links today (packet-switched, dedicated circuits, T1 and T3 carriers, fiber, satellite, etc.), these segments can be expected to embrace a variety of rapidly changing technologies at any given time. Once again, standard protocols and interfaces, including use of carefully selected gateways, will permit GTS to pass processing data from one UIS network to another, in as transparent a fashion as possible, thereby effecting truly global processing connectivity. The WAN segments must be capable of interfacing to both the interactive backbone LANs and the inter-complex backbone LANs, as well as embracing new communications technologies.

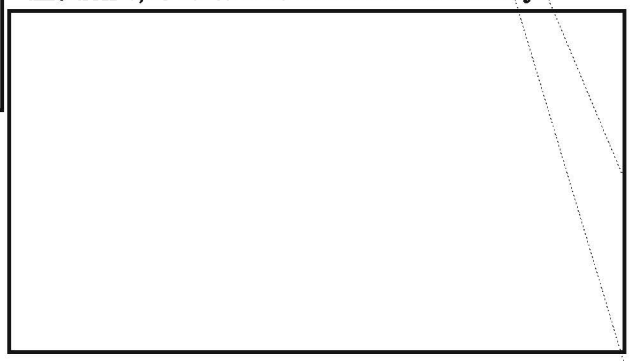
PLANNING AND BUDGETING CONSIDERATIONS

Cost Considerations

(U) Cost ramifications, both dollars and personnel, are necessarily an inherent part of the planning process, regardless of the issue being examined. Consequently, cost considerations will not be separated in this plan from other planning considerations. It must remain obvious, however, that affordability is the sine qua non for any aspect of planning, and that all cost factors must be considered in the planning process, including those (e.g. facilities) which are affected in the aggregate, but which are difficult to quantify as a function of a specific decision

Systemic Balance

~~(C-CCO)~~ The historic and on-going question of proper balance between collection and processing, both with respect to capability and resource commitments, is certain to continue indefinitely.



~~(C-CCO)~~

Equally important are considerations of having sufficient (i.e. neither too few nor too many) personnel with the proper skills and training in the proper locations to fully utilize the technical collection and processing assets available. Moreover, we must have sufficient and robust communications to ensure that whatever amount of data are collected can be moved in timely fashion to the point of processing. These considerations must be balanced also against such aspects as provision of the proper levels of support for equipment and personnel, regardless of location; proper facilities (to include power and cooling needs); and, more difficult to assess, the cost-effectiveness of modernization and asset optimization against the constrained investment resources which we must face.

Cost Drivers of Modernization

~~(S-CCO)~~ We must continue to move the SIGINT system forward to meet the ever-increasing challenges which it faces, but any form of progress has cost ramifications. Some of these cost-drivers represent simply the cost necessary to achieve a new, necessary capability. Others may represent the initial investment cost necessary to achieve improvements which have the potential of reduc-

ing costs, for a given level of capability, in future years. Still others represent potential cost savings, short-term, at the expense of some operational capability. All of these must be examined on a cost-benefit basis, based upon relative potential to fulfill our mission; timing of costs incurred (and the time-value of money); degree to which various resource expenditures equate to relative fulfillment of requirements; and to the timing of when given capabilities must be available. Typical cost-drivers to be so considered include the following:

- survivability (in all its aspects);
- computer security (to include networks and systems);
- need for pushing industry (via funded efforts) to advance technology in given areas to achieve the benefits of that technology earlier, instead of waiting for the technology to develop on the basis of market forces;
- benefits and drawbacks of attempts to achieve commonality (e.g. use of a single programming language such as Ada), and the extent to which such commonality should be mandated;
- effect upon facilities of new processing hardware which often takes up far less room, but requires far more power and generates far more heat;
- benefits (and cost savings) of preserving existing software (and the costs and problems of doing so) compared with the presumed later benefits of new, more standardized, more easily maintained rewritten software;
- loss of capability inherent in disestablishing existing, outdated systems compared with the benefits to be achieved in supportability, space, and compatibility with newer systems;
- benefits, drawbacks, and reasonable extent of use of standards, to include use of a common undercarriage for diverse systems;
- proper investment balance between general processing systems and infrastructure which support all organizations, and the need for improvements in particular operational areas;
- benefits versus cost and complexity of multimission processing systems, cross-correlation across collection types, and flexibility for use in varied scenarios (peace, crisis, and war); and
- cost-benefit analysis of various productivity enhancement programs, including personnel training and use of such technical developments as artificial intelligence and expert systems.

Organizational Considerations

(U) It can be argued easily that the current organizational structure of the Agency, not changed significantly in the last decade and predicated upon 1970's concepts of missions and roles, is already highly inefficient in dealing with our current problems. If unaltered, it is certain to become even more obsolete and ineffective in the years to come. Recent trends in technology and processing have had a particularly pronounced blurring effect upon the relevant roles of technical personnel in the Operations, R&E, and Telecommunications Organizations. There is already a great deal of duplication of activities across these key components, often at cross purposes and with little coordination or mutual visibility, and widespread misunderstanding of (or refusal to recongize) defined organizational roles. If left unchecked in the coming years of still more rapid technological change, we will be faced with a highly inefficient, immensely costly, technological anarchy.

(C) Careful analysis must be made of the proper roles of each organization with respect to current and impending processing technology; a partial reorganization may be desirable; and the defined roles must be understood and accepted by all. We will not be able to afford the levels of organizational autonomy which we have today, yet we must be very careful not to go overboard in defining roles to the extent that we are left with a stifling inflexibility of options. Of particular impact in these decisions are the ramifications of the current trends away from centralization and toward enhanced processing power at each analyst's desk. Although there is a potential for enormous gains in productivity and SIGINT output, there are also potentially many problems, most of which have been ignored heretofore. It must be realized that analysts are not trained programmers; that the efficiency of use of their workstations, as processing tools, will be substandard; that there will be widespread duplication, with little reusability, of software pro-

duced; and that little regard will be given toward maintainability, adherence to standards, and other precepts of good programming practice. The extent to which these aspects should affect rules, roles, and organizational structure cannot be foretold without detailed study. Nonetheless, it is essential that such areas be addressed, rather than the current practice of simply ignoring the problem and letting changes evolve without a concerted plan.

Summary

~~(C)~~ We must recognize that there has been an irreversible change in the way in which processing is accomplished; that continued change is certain; and that responsiveness in a purely technological sense is insufficient. A flexible plan, regularly revisited, is needed to ensure that our organizational, procedural, regulatory, and personnel practices are responsive to the changes.

Author's Note:
This paper was written three years ago; prior to the breakup of the Soviet Union; prior to the recent DDO restructuring; prior to the current emphasis on downsizing; prior to Paul Strassmann's CIM initiative; and without knowledge of the past three years of technological innovation. Nonetheless, its basic precepts appear to be nearly as relevant today, and the crystal ball of 1989 appears not to have been very murky.

Letter

To the Editor:

Another reply to the article, "Where was the Bogeyman?":

Hysteria over "the Islamic threat" is grounded in ignorance of the Arab peoples, their religion, and their culture. A close examination of all three would reveal a society whose basic beliefs and values are not dissimilar to our own. It would also highlight the individuality of the Islamic sects in the Middle East and their desire to establish national identities—factors that make a jihad unlikely.

It may be that the word "Islam" and "terrorism" are so linked in the minds of Westerners that we are unable to distinguish between the two. There is no doubt that terrorists have used and continue to use Islam as a pretext for their actions. The terrorists do not, however, speak for the majority of Muslims. We need to listen to the voices of the majority—not the over-publicized shouts of the extremists.

In any debate on Islam there are legitimate issues to address. We need to understand the reasons for the spread of Islam and the appeal that extremist groups hold for some Muslims. It would be a mistake to allow fear or hatred to distort our understanding, or to let the actions of a few blind us to the legitimate concerns and problems of the many. Only by objective analysis, and by laying aside our Western biases, can we hope to achieve progress in East-West relations.

[redacted] *B732*

~~FOUO~~

P.L. 86-36

P.L. 86-36

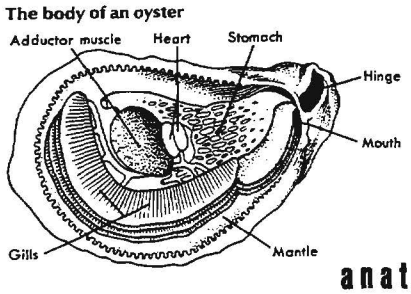
[redacted] *P05/SAO*

Missions/ Functions/ Organizations/ Personnel

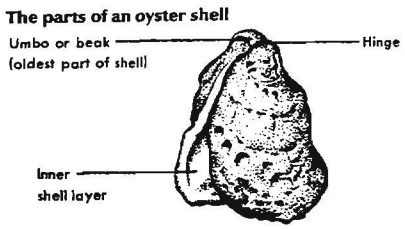
~~(C-CCO)~~ Questions often arise concerning the classification of NSA's missions, functions, organizations, and personnel. The following is a list of items and the classification, if any, of each.

FACT OF	CLASSIFICATION
• NSA's missions of SIGINT, INFOSEC, or OPSEC training	UNCLASSIFIED
• Information revealing the general missions and functions of COMINT activities without revealing specific COMINT techniques, procedures or targets	UNCLASSIFIED
• NSA's organizational designators below key component level	FOUO
• NSA's use of supercomputers as part of its mission	UNCLASSIFIED
• NSA's total budget or individual line items	CONFIDENTIAL
• Total manpower strength of cryptologic community, NSA or SCEs	CONFIDENTIAL
• Individual job title and description that does not contain classified information requiring classification (NSA Reg. 10-11 provides unclassified job titles and descriptions)	UNCLASSIFIED
• The statement "cleared for TOP SECRET, Special Intelligence (or cleared TS/SI)	UNCLASSIFIED
• The statement "cleared for TOP SECRET, indocrinated for CAT III COMINT"	~~C-CCO~~

ON THE TAXONOMY OF THE OYSTER



anatomy of the oyster



P0541

P.L. 86-36

(U) Turn the clock back to 1,000,000 B.C., plus or minus three sigmas. Our ancestors had just accumulated enough little gray cells to work with.

(U) They looked around and marveled at nature. They made note of the cycle of the seasons. They made note of the progression of the heavens. They made note of the tides.

(U) And they noticed that some matter replicated itself and some did not. That was a step in taxonomy: animate and inanimate, though they might not have used those terms.

(U) Then they also noticed that some of the replicable matter moved under its own volition, and some did not.

(U) People move at will on land, birds in the air, and fish in the sea. So, therefore, they must fall in the same class—animate matter that moves at will. Then there is also replicable matter that does not move under its own volition. For example, trees and oysters. Our ancestors noticed that trees are rooted in the earth. They noticed that oysters are rooted on rocks under water. Therefore, trees and oysters must fall in the same class—animate matter that cannot move under its own volition.

(U) Just as trees and oysters are related, so are substitution systems and codes. Superficially, they appear to behave in the same way.

(U) But it wasn't until 980,000 years later that our ancestors learned about complexities in the oyster that distinguish it mightly from a tree. It did take a while for them to realize that it was a difference in kind, not in degree.

(U) It's not surprising, therefore, that it has taken us until now to recognize that substitution systems and codes differ in kind, not degree. Actually, it was known years ago, but as that knowledge was based on instinct it was set aside as unscientific.

BASIC CRYPTOGRAPHY

(U) Let us review cryptographic principles. In cryptographic systems, there are only two possible operations:

- substitution: replacing one character by one or more characters.
- transposition: rearranging the characters.

It's possible to apply both to a single message.

~~(C CCO)~~ So we see that, on the surface, it seems reasonable to assign codes and ciphers to the same

family. After all, the ***enciphering*** process is the same—replacement. In a substitution system, one plaintext character is replaced by one (or more) cipher characters. The process is similar in a code system. The plain text (called "the meaning" in codes) is replaced by cipher called a code group. Therefore, the two enciphering processes are similar.

(U) Now let us turn to the ***deciphering*** process, as cryptanalysis was called in the early days.

~~(C-CCO)~~ The critical factor that distinguishes code from substitution cipher is the matter of the plaintext component. And this difference is a difference in kind, as you shall see.

~~(C-CCO)~~ In a substitution cipher, the possible plaintext equivalents for each cipher component are finite: the cipher letter can become one of only so many possible plaintext letters. It does not matter whether the plaintext component is only letters, or only digits, or a mix of letters and digits, or a mix of letters and digits and punctuation. It's a closed system.

~~(C-CCO)~~ This is true whether the substitution system is monoalphabetic, or polyalphabetic; whether it is based on a hand system or a machine system; or, even, whether there are variants to suppress the plaintext frequencies The possibilities for plaintext values are finite and known. If the enciphering process is complex—using shift registers or true one-time pad, for example—recovering the plain text correctly may be exceedingly difficult or even impossible; nevertheless, the cryptanalyst is confronting a system with a finite plain text population. The plain text must be "one of the above."

~~(C-CCO)~~ By contrast, in a code system, the possible number of plaintext equivalents (known as "the meaning") is very very large, for the plain text element may consist of a letter, digit, word, phrase, or sentence, or even, a complete message. Therefore, the possible plaintext values are, for practical purposes, infinite, and unpredictable as well. The nature of code is its high compressibility. For example, the plaintext component (the meaning) represented by a single ciphertext element (the code group) may be:

- a word: "treaty"
- a complete sentence: "This morning I had a long private conversation with the Prime Minister."
- a phrase: "under no circumstance"
- time: "1800 hours"
- a spell: "-Y-"
- a family of verb, abstract noun, agent noun, adjective, adverb, gerund
- a selector: "take fourth meaning of previous group"
- an oblique form of noun or verb: "would have signed"
- a place name: "Paris"
- a title "HR the Crown Prince of Ruritania"
- a ship: "the gunboat MAGNOLIA"
- an organization: "24th Battalion"
- deciphering instructions: "beginning with the next group use the PERSIMMON table."
- a complete message: "Attack at Dawn."

(U) So as you can see, unlike a substitution system that consists of a finite plaintext population, in a code system the plaintext possibilities are virtually infinite. For that reason the meanings cannot be recovered by purely statistical means, though statistics plays a part in the recovery of the meanings.

• study past traffic and combine frequent clichés such as "Reference your message Number 364" as one group. (Except you have unexpected subjects like Boris and Gorby, and narcotics interdiction, and Bosnia and Hercegovina, and GATT . . .)

(U) And then there is the famous case of a French World War I compiler who organized the codebook meanings by whether or not the nouns were derived from verbs—and this for a trench code!

THE FREE-WHEELING CODE CLERK

(U) To compound the difficulty of recovering the meanings of code groups, any rule the compiler sets for encoding plain text the code clerk may undo. Take, for example, a codebook that is in caption order—when the meaning is filed under the most important word in a phrase. If the caption is

1234 TREATY

thereafter you may see phrases incorporating TREATY:

1245 treaty of peace
1267 commercial treaty
1278 to sign a treaty
1289 the Queen signed the treaty

(U) The code clerk who is not familiar with the codebook very likely will encode the equivalent of 1289 as three groups, or even four:

Queen
Sign
(past tense)
Treaty

(U) And if the code clerk is looking for the number 1800, to measure distance (1800 kilometers) and runs into the military time 1800 hours first, that's what will be used. The decoding clerk at the other end knows to decode it as "1800 kilometers."

THE SYLLABARY

(U) Then we have the case of the syllabary, a gray area: these, like codes, should be catalogued separately as "syllabaries," not as substitution systems, for syllabary systems are open-ended and as unpredictable as codes.

WHY IT MATTERS

~~(C-CCO)~~ In the past we used to peruse hard copies of the system descriptions to learn about the past cryptographic habits of our targets. But now we're into information retrieval. If we're looking for a specific type of system, we must type in the appropriate term to access the database. And if we're looking for code, we will not find it, for codes are tagged as "substitution" systems. It's a loss of information that once was known.

(U) How did this state of affairs come to pass? I believe it was an excess of zeal in taxonomy, and misguided at that, with a large dollop of pedantry laced in.

(U) And this ties is in with recent practice.

~~(C-CCO)~~ Consider the term pentagraphic, used of a code (or cipher) group consisting of five characters. In parallel construction, one of twelve characters would be called dodecagraphic! We have puzzles enough set by our targets without concocting our own and confusing cryptanalysts who have not had the benefit of a classical education.

(U) It's time we dropped that clunky usage and reverted to that of an earlier, more elegant time, when a dodecagraphic group would be written as 12-character (or -digit-, or -letter, as the case may be). The important word in the compound—the length—is instantly recognized. And that's as it should be. Let our documentation be self-evident. Eschew polysyllabics.

(U) And on that note, let me invite everyone to drop forthwith the indiscriminant use of "superenciphered." Super means on top of. A code is "enciphered" using an additive, let's say. Period. Only if there is still another encipherment over the first should the term be "superenciphered":
• A 4-letter code enciphered with polyalphabetic substitution.
• A 4-letter code enciphered with polyalphabetic substitution, and superenciphered (ore "re-enciphered") by transposition.

(U) Isn't that neater?

(U) Let's get rid of the overburden of polysyllables.

(U) Keep it lean, mean, and clean.

P.L. 86-36

Valedictory

[redacted] Z5,
Formerly Chief, P1
CRYPTOLOG *Publisher Emeritus*

Address at a luncheon on 31 January 1992 to commemorate P1's 30 years of service.

(U) We were all saddened by the recent death of Bill Lutwiniak, but we know he would have wanted us to commemorate the occasion for which we are gathered. So today we dedicate this proceeding to his memory, and I ask that you join me in a moment of silence.

~~(FOUO)~~ P1 came into being, as nearly as I can ascertain, on Flag Day in 1961 as part of an NSA reorganization. John Kennedy had been in office only a few months and there was a mood of excitement in the country, tempered by an apprehension caused by the cold war and the potential Soviet menace. After all, part of the reason we reorganized was because of Martin and Mitchell. No more would we be ADVA, ALLO, GENS, or MPRO, but we would be A Group, or B Group, or G Group. How mundane!

~~(FOUO)~~ I was a young analyst in GENS which became A4 and very little changed for me. I had never even heard of P1. [redacted] who is here with us today, was appointed the first chief. He was chief for about a year. I got to know Dale later when he was chief of C, I believe, and when he helped G4 get a computer. He was succeeded by Frank Raven. Once of the things that happened while Frank was chief of P1 was the start of the cryptomath program in 1963 just as I was signing up for a new job in P1. I tried to get into the CMP, but Frank said I had been at the Agency too long, and he assigned me to work with Glenn Stahly in G4. By then, Lyndon Johnson was president and the world situation continued to be bleak.

~~(FOUO)~~ After about a year in G4, Mr. Raven told me I had a choice: stay in P1 and move to A5, or, if I wanted to stay in G4 I would have to transfer there. Since I was in the middle of a major project I opted to stay in G4, and my association with P1 became a lot less for the next 20 years.

~~(FOUO)~~ For a while, Ted Leahy helped me on my projects. Then he stopped coming by, and one day, seeing him in the hall, I asked him where he had been. He said he was helping people who needed the help more, that I didn't need him anymore. This was not exactly true, but it does reflect the P1 spirit and what it represented.

~~(FOUO)~~ In the meantime, George Vergine and Art Levenson—neither of whom, unfortunately could be here with us today—were the 3rd and 4th chiefs of P1 for about 7 years between 1966 and 1973. Nixon was President and Watergate consumed the nation.

~~(FOUO)~~ I had gone to GCHQ in 1971 on a G4 billet which was created because P1 would not let me be on their billet, which at the time was reserved for CMP graduates. I returned to the states in the summer of '74, and my family and I watched the hearings on Nixon from our motel room on Route 3 in Bowie, and later, listened on the radio to Nixon resigning while we were sitting in our empty house awaiting our furniture.

~~(FOUO)~~ At that time Bill Lutwiniak was in the second of his eight years as Chief of P1. This was the longest time for any of the chiefs of P1. I hope some of the speakers will talk about those years because I really had no direct dealings with P1 during all the years between 1965 and 1985 except through the CMP. P.L. 86-36

~~(FOUO)~~ When Bill retired, he was succeeded by [redacted] as the sixth Chief of P1. Ford, Carter, and now Reagan occupied the White House and the country's cold war continued without much change.

~~(FOUO)~~ During the 80's there was tremendous growth in the Agency, both in dollar and manpower allocations. I was still in G4 and experienced this enormous influx of new people into our already cramped quarters. It was, nevertheless, an exciting time, and we were accomplishing a lot of miracles, as [redacted] liked to say. So it was with some reluctance and misgivings that I accepted the job as the 7th Chief of P1 in 1987. Soon after, George Bush became the 7th president in the same 30-year period. I am not trying to draw a parallel between any one chief of P1 or any president; just that there were the same number.

P.L. 86-36

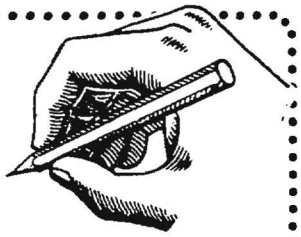
~~(FOUO)~~ Now the world scene was radically changing, and austere times were in store for almost everyone. The demands for restructuring were everywhere, and with the recent collapse of the Soviet Union, the reorganization, which had been planned for two years, raced towards completion. As the restructuring took shape, it became clear that a P1-like organization was not appropriate in a functionally aligned DDO.

~~(FOUO)~~ Now we enter a new era, and from my perspective, it will be exciting. About half of the old P1 will be going to the new Z Group, with some of the functions and individuals dispersed. The CMP will remain intact and unchanged in Z5 which I am heading. Other parts of P1 will survive in various other groups and the new operations staff.

~~(FOUO)~~ It is wonderful to see so many people, both present employees and retired P1'ers who have come out today to pay tribute to this wonderful organization. It is now time to hear from some of the other people who made P1 what it was in the past.

~~(FOUO)~~ In closing, while we salute the old, I leave you with the thought that it is people who make institutions great. We have not lost that magic ingredient with the demise of P1, so let's go forward and remember:

(U) "These are the good old days!"



To the Editor:

The Government Code and Cypher School was formed under the control of Cdr. A. G. Denniston. In 1938 Denniston was preparing for war, and encouraged the Foreign Office to buy the property at Blechtley Park. It had several advantages: 45 miles from London and 50 miles from Oxford and Cambridge, where Denniston hoped to recruit most of the mathematical and linguistic specialists. When war broke out, everything was in order, and scholars from the universities were rapidly recruited. For a short while the staff could be accomodated in the large country house, but soon it became necessary to build huts where various sections were housed—Hut 5 for the Italian Army cyphers, and others for weather and similar subjects. Many of the sections and huts have long been identified, but there were a few where top secret work was done, so secret that it was not until 1973 that Group Captain Wintherbotham made it known that teams at Bletchley had broken the German High Command cyphers—the Enigma.

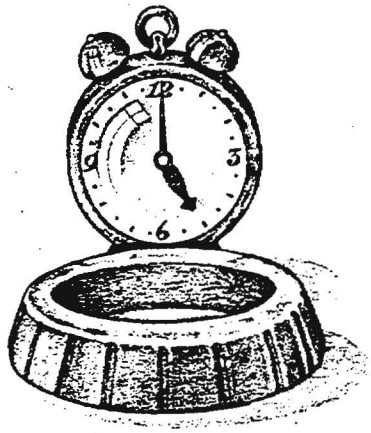
The chief hut for this work was Hut 6, and to this day, it still stands. But Bletchley Park is slated for development, and the remaining huts will be bulldozed.

As many of those who worked in Hut 6 and elsewhere in Bletchley have objected to the disappearance of Hut 6, the Bletchley Park Trust has been formed. Already much has been done. It is likely that the Government will halt the demolition.

The Trust would like to hear from those who have an interest. The Trust may be reached at Suite 8, Denbigh House, Denbigh Road, Bletchley, Milton Keynes, Bucks, MKI 1YF. The chief executive is Ted Enever.

William Filby, former member, GC & CS.

A Visit to TIME



P.L. 86-36

Reported by: [redacted] *P05,* et al.

For some time agency reporting specialists have suggested adapting the organizational structure and publication techniques used by print journalism. In an effort to see which of these techniques can be used in agency reporting, a group of senior reporters visited TIME magazine on 17 and 18 June 1992.

P.L. 86-36

Persons Visiting: [redacted]

We were very openly and hospitably received by senior officials of TIME, Inc: the TIME Magazine Managing Editor, the Deputy Managing Editor, the Editorial Operations Director; two Senior Editors; the Picture Editor, and others.

From the very first, TIME insisted that we spend two days with them. They wanted us to see the progression of articles through the editorial process from one day to another. On both days we were privileged to sit in on the 1000 a.m. editorial session that the Managing Editor held with his key staff members to discuss ideas for the weekly issue of TIME Magazine, the status of articles already underway, etc. At these one-hour meetings the senior leaders of TIME, in concert with key staff members, decide what story lines will be pursued by the magazine. This is an intentionally free give-and-take regarding both domestic and international topics.

The morning session is followed by a series of additional section-level editorial meetings. It is at these meetings that TIME managers direct the reporting effort, channeling and focusing the various story lines. Once the actual article is written, there are quality checks throughout the production process by researchers, fact checkers, and copy editors.

In separate sessions, the Managing Editor and his deputy told us that what we witnessed in these editorial sessions was not always the procedure for TIME. Not too many years ago, it was a top-down structure, with the top telling the bottom what articles should be written, and even at times, the ideological thrust of those articles. This was particularly true when Henry Luce owned the magazine.

Now, stress is put on bottom-up collegial communications. This has not been an easy process for TIME, and both the Managing Editor and the deputy emphasized that one has to have patience in implementing such a process. They told us that some managers and employees feel more comfortable with a top-down structure. There is still some hesitancy among the staff to be openly contributory. But they say that the bottom-up approach is definitely the right one, because for the magazine to compete successfully these days, it has to have the fresh ideas and the proprietary involvement of its employees. We were struck by the similarity of the problems facing TIME and our own evolution toward a lower-echelon decision-making and employee-involved Operations

Directorate and Agency.

TIME has about 400 persons to carry out its weekly publication; this does not include another about 200 who are involved in the business end—subscription handling, etc. Junior reporters start at about $35,000. There aree 28 bureaus, with about 55 correspondents outside New York. Henry Cabot Lodge was their first correspondent.

TIME does not have a formal training program for their reporters. They expect individuals whom they hire to already be trained journalists with experience gained elsewhere. Their staff is composed of experienced individuals trained in the journalistic style of reporting. They are required to follow the "TIME style" of writing. The deputy editor kindly gave us a few copies of "Writing for TIME", which is their internal style manual.

There is a Wednesday afternoon critique session, but there are many quality checks all along the line throughout the production process.

Researchers are used to assure that the facts are right in an article. TIME does not have a formal training program, except for training some persons on new equipment received. They do not train their reporters and writers. The deputy manager told us that it is still a "buyer's market" with TIME having their pick of young people anxious to come to work for TIME. He said this stems from the interest in journalism generated by the Watergate case.

Their final product is disseminated to numerous CONUS (e.g., Philadelphia, Atlanta, Wisconsin, Illinois, Dallas, Los Angeles, San Francisco) and four overseas locations for printing. The international edition is different from their domestic edition, and ads are matched to the various regions of the world.

We were told that within the U.S., even individual subscribers receive different ads in their issue of TIME. Depending upon facts related to a specific subscriber, a computer determines what ads to include in a particular issue: things like age, sex, ZIP code, salaries, etc., are used as the basis for determining the make-up of the individual copy. This amazed all of us, and we were wondering if there were some application of this software that we could apply here. TIME offered to discuss it further with us, if we desired.

Most of their non-management employees belong to a union, the Newspaper Guild, so like those of us in the federal service, TIME is not as free to hire and fire as one might think, we were told.

A large number of their employees work three days a week, twelve hours a day, and like it. This has to do with the natural production pressure that builds on Thursday and does not end until about 0300 Sunday morning when everything has to be electronically sent to the printing and distribution points. About 80-90% of the work is done on Thursday and Friday, with the crescendo coming between 3 pm Saturday and 3 am Sunday. The goal is to have the magazine on the street early Monday morning. When asked why Monday, they told us that this is just the way it has evolved over the years. Long, pressure-filled hours are normal during this time.

About 80% of the foreign bureau personnel are U.S. nationals, with foreigners hired to handle the clerical and administrative matters.

As for technology, the Managing Editor told us that the TIME goal is to have Macintosh terminals for everyone, with the ability to do article preparation on the terminal, and transmit to a large number of other terminals. At present they use a variety of computer terminals. Eventually, all the Macintoshes will be part of a single network so that article preparation and transfer of material can easily be accomplished from reporter to editor to photo desk, and so on. They plan to abandon their present ATEX system (a company name, we were told, which does not expand). We were told that a company named Stratus was great for preventing any down time in their vital operations.

As in nearly all news magazines, photo and graphic design play a large role in each issue. Once a story line is decided upon, photo taking and selection is usually done before an article is completed. TIME has independent photo journalists under contract as well as access to an electronically delivered photo service, similar to the

AP or Reuters wire. TIME is implementing a new high-resolution National Digital system which will enable them to quickly receive and incorporate photos into their magazine.

The art director decides the layout. Three or four of the picture editors are also photographers. Magazine covers are planned as long as eight weeks in advance, unless some special event, like the Los Angeles riots, occurs.

We met the individual who is responsible for TIME covers. Just 12 years ago, he said, TIME was a black-and-white publication. In 1981, they went to six pages of color, and finally in 1984, went to all color.

Actual readership is a lot higher than the sales number, because they know from surveys that copies are read by approximately four persons beyond the person to whom the magazine is addressed. They estimate a 30-million readership weekly.

Every article in TIME is carefully read by company lawyers to see if the magazine could be liable for something written. The managing editor estimated that the magazine has about one serious suit per year.

We will be reviewing our trip to TIME and to other publishers to determine what we might use to improve our reporting at NSA. We are particularly interested in generating greater interest in the editorial-board approach to production.

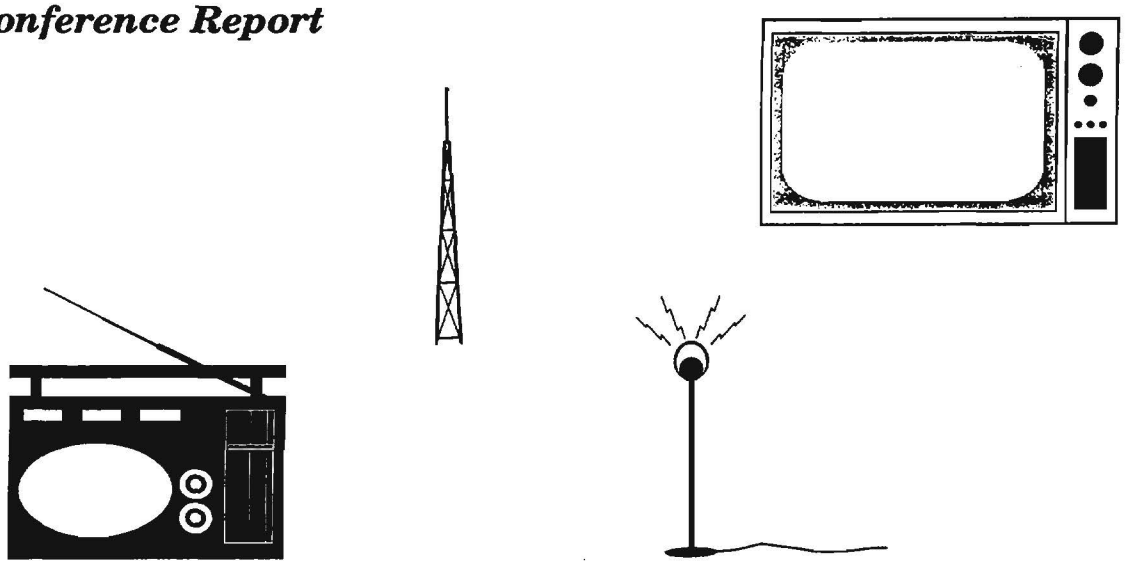
Electronic Publishing Quiz

Expand the Acronym

1. AFP _____
2. APA _____
3. CALS _____
4. CRT _____
5. DJDE _____
6. DOS _____
7. DPI _____
8. FDL _____
9. GML _____
10. JCL _____
11. JES _____
12. MICR _____
13. OCR _____
14. OGL _____
15. PDL _____
16. PSF _____
17. RFT _____
18. SGML _____
19. WYSIWYG _____
20. XES _____

Answers on page 14

Conference Report



(U) 1992 National Association of Broadcasters Convention and Exhibition; The Annual Broadcast Engineering Conference; and HDTV World '92 Conference and Exhibition; held concurrently in Las Vegas, Nevada, 12-16 April 1992.

P.L. 86-36

Reported by: [redacted] *P054 S/A*

~~(C)~~ The primary purpose of this trip was to provide me with the opportunity to assess current and emerging broadcast, video, teleconferencing, and multimedia technologies associated with the Operations Directorate dissemination initiatives [redacted] and other associated publication projects.

(U) Second, the trip provided the opportunity to assess new broadcast related digital, encryption, and laser technologies and continued escalating foreign interests in visual information production, hardware, and distribution technologies.

P.L. 86-36

~~(C-CCO)~~ Third, the knowledge gained from this trip will further assist the Operations organizations and Agency support organizations in developing new intelligence dissemination opportunities in video and multimedia technologies, and aid in the assessments of front-end SIGINT collection opportunities.

~~(FOUO)~~ Fourth, the NAB provides a unique assessment opportunity for those Agency employees involved in implementing the NSA/CSS Visual Information Services Working Group Report of November 1991. Information gleaned from NAB seminars and exhibitions will assist me in developing and maintaining a "state-of-the-art" understanding of facility planning and design, facility management, reporting production techniques, storing and retrieval techniques, archiving techniques, and technical equipment integration.

CONFERENCE OVERVIEW

(U) This annual convention and exhibition continues to be the largest of its kind in the world, and continues to grow with a record number of over 52,700 registered attendees and exhibitors, and a record international attendance of more than 8,651. International attendance reflected an increase of over 20% from NAB '91. New technologies, software developments, recording formats, and multimedia applications continue to be exhibited.

CONFERENCE SEMINARS

(U) NAB seminars were divided into Engineering, Radio, Television, and HDTV categories. In an effort to get a flavor of diversified areas of interest, I attended the following seminars:

Engineering Sessions

- Interactive Video , The Birth of an Industry, TV Answer, Reston VA
- The In-Touch TV System, A Technology Description Interactive Systems, Beaverton, OR

- Production Processes for Interactive Television Interactive Network, Inc. Mountain View, CA

- Pay Per View-Video on Demand, Jerrold Communications, Hatboro, PA

- Update on New Interactive Television, Applications of T-Net Radio Telecom and Technology, Inc. Perris, CA

Video Production & Post Production

- Driving Towards PC-Based Post Production, Autodesk, Inc. Sausalito, CA

- Bridging Computer Graphics and High Quality Video Tektronix, Video Products Operation Wilsonville, OR

Television Sessions

- Controlling Our Future, Broadcasters, Cable, Telco

- All-Industry Luncheon with addresses by Eddie Fritts, NAB President/CEO; Topic: Strategic Planning and Innovation (The Armed Forces Radio Television Service was honored), and by Former President Ronald Reagan, Distinguished Service Award Recipient (Ironically, I witnessed a second attack on this President at a Hilton Hotel, this time as he delivered his NAB keynote address.)

- Law and Regulation Conference Luncheon, Alfred C. Sikes, Chairman of the FCC. Topic: The Future of Broadcasting, Merging of Technologies, Need for Adaptability

PERSONS VISITED

(U) David Lyon, Chairman, CEO Basys Group

(U) Comments: Basys Automation currently has a system installed in the T5 Media Center area. Basys CEO provided insights for future business areas and technologies that the company is actively pursuing in information management systems and services related to video production, databases, library and archive, and multimedia technologies.

(U) Jean Gard, Entertainment Industry Segment Manager for Digital Equipment Corporation (DEC)

(U) Comments: Ms. Gard shared insights for future business areas and related technologies that DEC is actively pursuing related to multimedia technologies and services.

(U) Geoffrey S. Roman, Vice President, Technology and New Business Development for Jerrold Communications, a division of General Instrument Corporation

~~(C-CCO)~~ Comments: Mr. Roman is a former MITRE principal. In his public NAB engineering presentation, Roman mentioned that TCI and US West are using cable distribution technologies. Roman predicted major domestic US telecommunications implications in six to nine months. Although Roman did not go into detail with this statement, I believe Roman alluded to a potential new business enterprise for US Cable Companies in the telephone and data business in direct competition with the Baby Bell companies. After his formal talk he gave an interactive video engineering presentation

~~(FOUO)~~ Representatives from the National Cryptologic School's Visual Information Services Facility, E23, Research and Engineering, R8, and the DIA J2 Defense Intelligence Network (DIN) executive production staff.

~~(FOUO)~~ Comments: This provided an excellent opportunity for informal management and technology networking between NSA/CSS elements as well as interagency liaisons.

CONFERENCE ASSESSMENTS

Telecommunications Policy and New Technologies

(U) The FCC, through the dynamic leadership of its Chairman and proactive Commissioners, is continuing to drive the US into world leadership in digital communications. Featured at this year's NAB was the first over-the-air broadcast of digital HDTV on experimental TV Channel 15 as authorized by the FCC. (For those of you who have not seen demonstrations of HDTV, the image quality

will knock your socks off. It will revolutionize the broadcast and entertainment industries, not to mention what it will do to the telecommunications industry because of digital technology, video compression techniques, and non-video digital services.) The FCC anticipates announcement of a US digital TV broadcast standard in 1993. Shortly thereafter, US broadcasters are positioning to rapidly enter this new market opportunity. Digital AM and FM radio has already been developed. Digital data services are positioning for the radio market and new receivers will soon be installed in US-sold autos to provide alphanumeric information.

~~(FOUO)~~ Many international NAB attendees continue to assess and procure US developed video production and distribution technologies for a variety of entertainment, business, government, and military applications. The NAB has reached such an international scope, that the US Department of Commerce and Foreign Money Exchanges maintain sizable on-site convention presence.

Hardware

Video Production

(U) Off-the-shelf hardware technologies continue to develop for both linear and non-linear video production. Linear technology allows only ordered video production, i.e. item #1, then #2, then #3 and so on. Non-linear technology allows immediate random access broadcast quality video production, much like a word processor. Analog motion video, analog still images, and analog voice narrations are first digitized in non-linear editing and then randomly manipulated to produce a final video product. You can cut, paste, and transition combinations of both audio and video using computer technology, control software, an icon control screen, and a special-purpose mouse developed to expedite video productions.

(U) Television cameras and video recorder devices are both moving to digital technologies with approximately 1000 lines of resolution. As these digital devices develop, they will expedite the non-linear video production process because raw materials for video and multimedia productions will already be in a digitized format. I certainly believe non-linear video production is the way to go in the future. However, because this developing technology is expensive, I recommend using linear video production technology until the market settles a bit and there is a wider selection of vendors and established vendor standards and interfaces.

Video Recording

(U) New tapeless video production formats include rewriteable optical disc and rewriteable magneto-optical disc. Manufacturers exhibiting this equipment at the NAB included Panasonic, Pioneer, and others. These video recording formats support both linear and non-linear video production, storage and retrieval, and archiving requirements. These optical technologies are currently limited to approximately 55 minutes to 2 hours of record/playback time, depending on the manufacturer as well as analog, digital, and compression formats. The optical recording media is quite expensive when compared to videotape. Example: a one-hour Beta-CAM SP broadcast quality videotape costs about $25 versus a one to two hour magneto-optical disc which costs about $1200.

Duplication

(U) A high speed VHS duplication system was exhibited for the first time by The Sony Corporation. Other manufacturers including Sony, Panasonic, and others exhibited a number of real-time duplication systems, some with auto cassette feeds.

Teleconferencing

(U) Fully assembled teleconferencing units and integrated teleconferencing technologies were not featured at this convention. However, a number of manufacturers and system integrators exhibiting at the NAB offered such systems.

Software

~~(FOUO)~~ Software development is not currently a strong point for video hardware producers. Although a diversity of off-the-shelf hardware solutions exist for video SIGINT production, storage and retrieval of motion video and still images,

and long term archiving, at this point, I anticipate some limited software machine control development with a hardware vendor or related broadcast software developer to maximize automation capabilities of existing commercially available off-the-shelf hardware systems.

~~(FOUO)~~ There is currently no software standard for desktop video production. As in word processing, a number of software suppliers provide unique applications programs. Important to note is the fact that mouse hardware technology is being reworked for video production. Video editors using computer mouse technology for video production are not happy with current mouse designs for speed, hand-eye coordination, and physical durability.

~~(FOUO)~~ Several vendors are working toward software that will combine scripting, database searches, production, and machine automation control. This software development will greatly increase the flexibility of video production facilities.

Encryption

~~(C)~~ A number of companies are currently manufacturing and selling commercially available off-the-shelf analog and digital video encryption devices. These companies include: Leitch, Macrovision, Scientific Atlanta, and Sony. Sony, among others, now offers an international teleconferencing network.

Transmission

(U) Canon Broadcast Equipment Division introduced a new Optical Beam Communications System called the Canobeam. The NAB Broadcasters Daily News reports that this laser devise, using a high-speed modulated optical beam, can transmit up to eight video signals and 18 audio signal channels in both directions. Canobeam transmits wide-band signals up to 500 MHz. Data can be sent at speeds up to 156 Mbps. Transmission distance can range up to 2 km, and digital data transmission distance can be increased without signal degradation by using the Canon 3R function relay. (Can you imagine this type of technology in the next war?)

CONCLUSIONS AND RECOMMENDATIONS

[redacted] EO 1.4.(c) P.L. 86-36

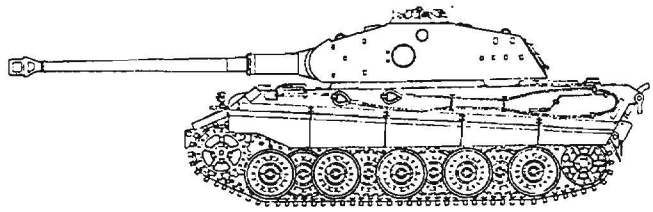
[redacted] (The NAB and the US Department of Commerce maintain records of overt convention participation by name and country.) P.L. 86-36 EO 1.4.(c) Commercially available off-the-shelf technologies supporting visual information (VI) production, teleconferencing, and encryption continue to be exported to foreign countries for diversified multimedia information flow capabilities.

~~(C)~~ The Operations Directorate should continue representation at conferences, conventions, and expositions, such as the NAB, which will enhance the knowledge base required for the management, production, engineering, exploitation, teleconferencing, and multimedia development of cryptologic visual information (VI) activities.

(U) In order to adequately cover the growing magnitude of the NAB Convention, Exhibition, and Engineering Conference, I recommend expanded Operations Directorate representation, and I encourage representation of other Key Components at future conferences in support of expanding requirements for Agency Visual Services.

(U) New for 1993, the NAB announced a premiere conference and exhibition called "Multimedia World: Merging Video, Audio, and Computers." Beginning next year, this new annual event will be held concurrently with the NAB Convention and will provide a new forum for post-production video, business video, computer professionals, and broadcasters.

A Sidebar to SIGINT History



Betty Wanat, Rct.

~~This article is classified TOP SECRET UMBRA in its entirety~~

In early November 1977, the political situation between Ethiopia and Somalia had reached a crisis. At the same time the American Embassy reported that Ethiopia was considering breaking relations with the United States, though Ethiopia needed the food and equipment that the US had been providing.

Towards a Viable Tech Track

To whom it may concern:

Towards a viable tech track I hereby offer some suggestions.

• Establish a program of post-professionalization rotational tours.

• Sharply increase the proportion of promotions awarded to tech trackers. It is the traditional way: the more opportunities for advancement, the more enticing the prospect for remaining a tech tracker.

• Add to all promotion boards a voting tech tracker who will look out for other such.

• Convert some of the SCE slots to SLEs. We will be needing even more technical experts in the future.

• Be generous about sending tech trackers to professional conferences. The insights that can be gained are invaluable. In our closed society a breath of outside air is absolutely necessary. What's more, the attendees can share the wealth by writing up a conference report for CRYPTOLOG!

• Allow tech trackers time to document their projects at their conclusion. Documentation should be an integral part of any professional's duties.

• Give due credit to people who pass on the torch. These are the people who document their knowledge and techniques for coming generations, who act as technical mentors to interns and to seasoned analysts as well, who develop courses, who teach and lecture, who develop the professional examinations and grade them, who write philosophical papers on futuristics in their discipline, who compile lexicons and working aids of all kinds. They provide the hard core of technical and historical continuity.

• Honor the technical types who manage peopleless projects rather than people. Let's take a look at our own resources in these tight budget times. We are wont to make heavy weather about managing a long-term, big-bucks project. But we already know from the write-ups of the productivity awards that we have gifted people who can knock a complex project off in no time flat, and on a shoestring at that. Reward them suitably.

• Do not overlook the technical staffers. These are the people who fight the dragons that besiege our gates for secrets. We depend upon them to devise an unimpeachable defense for retaining classification.

• Be very very careful about overriding an evaluation of a tech tracker that is done by a technical board. If you think it necessary to do so, explain your reasons to the technical advisors.

• Last, but not least, about TQM: cumulatively, our professional cadres have a lot of smarts, imagination and ingenuity. Sound them out. Use them to solve problems.

Editorial Policy

CRYPTOLOG is a forum for the informal exchange of information by the analytic workforce. Criteria for publication are: that in the opinion of the reviewers, readers will find the article useful or interesting; that the facts are accurate; that the terminology is correct and appropriate to the discipline. Articles may be classified up to and including TSC.

Technical articles are preferred over non-technical; classified over unclassified; shorter articles over longer.

Comments and letters are solicited. We invite readers to contribute conference reports and reviews of books, articles, software and hardware that pertain to our mission or to any of our disciplines. Humor is welcome, too.

Please note that while submissions may be published anonymously, the identity of the author must be made known to the Editor. Unsigned letters and articles are discarded.

If you are a new author, please request "Guidelines for CRYPTOLOG Authors."

How to Submit your Article

Back in the days when CRYPTOLOG was prepared on the then state-of-the-art, a Selectric typewriter, an article might be dashed off on the back of a used lunch bag. But now we're into automation. We appreciate it when authors are, too.

> *N.B.* If the following instructions are a mystery to you, please call upon your local ADP support for enlightenment. As each organization has its own policies and as there's a myriad of terminals out there, CRYPTOLOG regrets that it cannot advise you.

Send two legible hard copies accompanied by a floppy, disk, or cartridge as described below, or use electronic mail. In your electronic medium (floppy, disk, cartridge, or electronic mail) please heed these strictures to avoid extra data prep that will delay publication:

- do not type your article in capital letters
- do not right-justify
- do not double space between lines
- but **do** double space between paragraphs
- do not indent for a new paragraph
- but **do** paragraph classify
- do not format an HD floppy as DD or vice-versa–our equipment can't cope
- label your floppy or cartridge: identify hardware, density of medium, software;
- put your name, organization, building and phone number on the floppy or cartridge

The electronic mail address is *via* PLATFORM: cryptlg @ curator
or *via* CLOVER: cryptlg @ bloomfield

CRYPTOLOG publishes using Macintosh and Xerox Star. It can read output from the equipment shown below. If you have something else, check with the Editor, as new conversions are being added.

SUN	60 or 150 MB cartridge	ascii only
XEROX VP 2.0, 2.1	5 1/4" floppy only	
WANG		Stand-alone or Alliance
Macintosh	3 1/2" DD disk only	Please furnish a copy in TEXT as well as in your software, as we may not have all the software upgrades
IBM & Compatibles	3 1/2" DD or HD 5 1/2" DD or HD	Please furnish a copy in ascii as well as in your software, as we may not have all the software upgrades