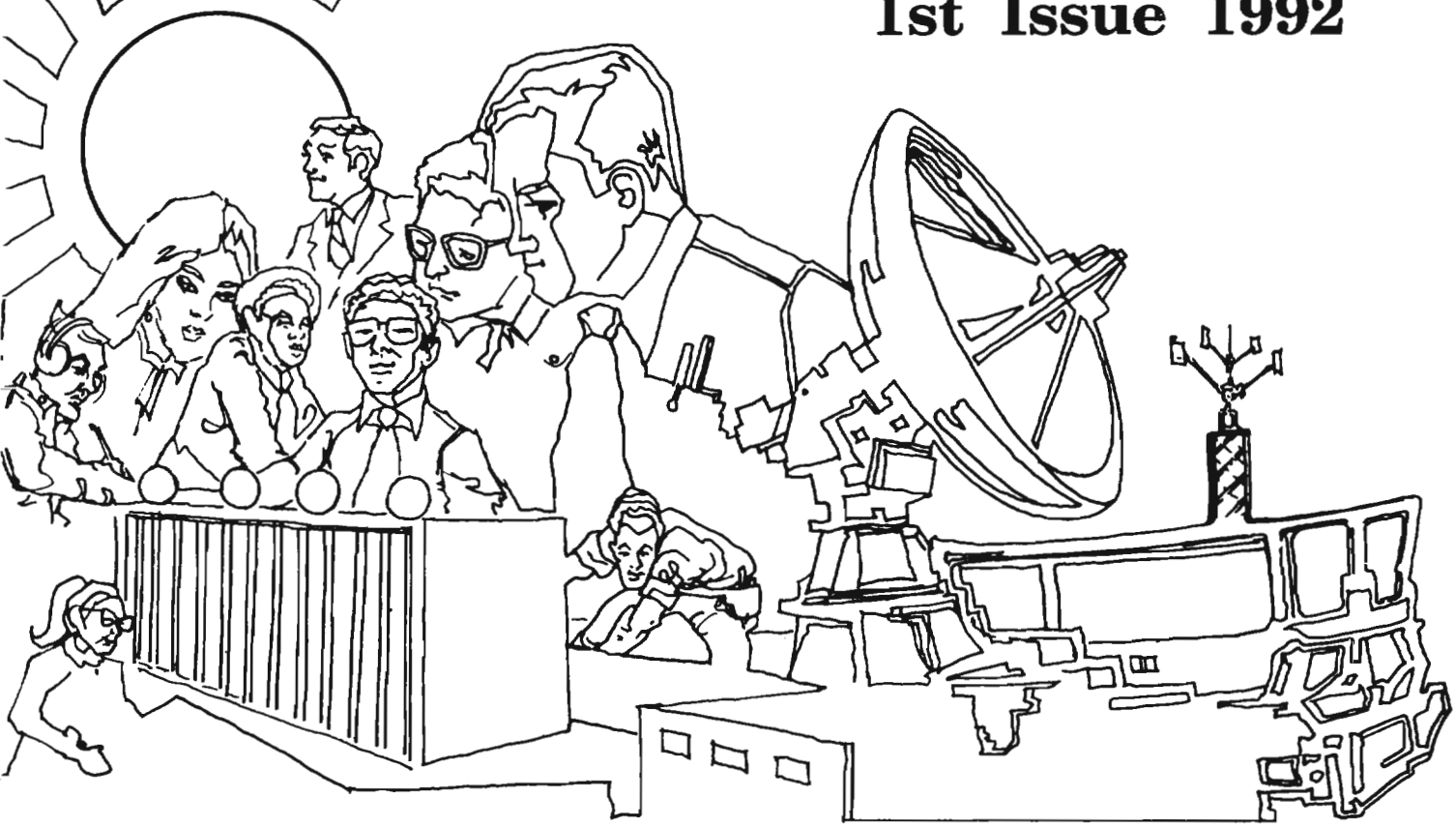
~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

1st Issue 1992



UNDER NEW MANAGEMENT	[redacted]	1
THE GREAT CONVERSATION	[redacted]	2
OPSEC AS A MANAGEMENT TOOL	[redacted]	7
WHERE WAS THE BOGEYMAN?	[redacted]	10
THERE NEVER WAS A BOGEYMAN	Peter D. Molan	13
SANDLOT	[redacted]	15
THE ALMANAC APPROACH	[redacted]	17
FURTHER TO 'THE TEN MOST WANTED'	[redacted]	22
NL: IN MEMORIAM	Doris Miller	22
CLASSIFYING YOUR PERSUM	Richard Sylvester	23
SHELL GAME	[redacted]	24
LETTER		24
SIGINT IN THE NOVELS OF JOHN LE CARRE	[redacted]	25
TECHNICAL LITERATURE REPORT	[redacted]	33
CONFERENCE REPORT: ITCC '91	[redacted] et al.	34
FROM THE PAST		42
EDITORIAL		43
GOLDEN OLDIE		44
TO CONTRIBUTE		45

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. 1 . . . . . 1st Issue 1992

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
via CLOVER: cryptlg @ bloomfield

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

~~FOR OFFICIAL USE ONLY~~

UNDER NEW MANAGEMENT

[redacted] *P05, Prop.*

(Successor to [redacted] *Publisher Emeritus, Z5, late of P1)*

P.L. 86-36

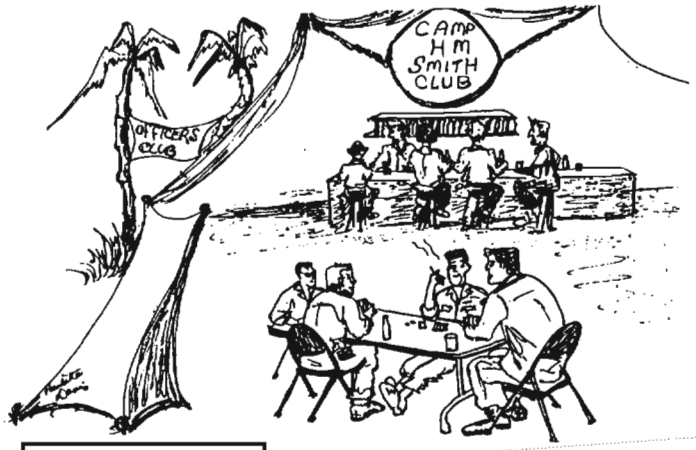
The recent restructuring of the Directorate of Operations has landed many people in new places. I'm delighted to report that one such change is that [redacted] the editor of CRYPTOLOG, was reassigned to P05. That, in turn, puts me in the position of publisher of CRYPTOLOG.

It's a pleasure to be associated with this friendly journal. With its mix of technical, expository, philosophical, futuristic, argumentative and historical articles—with a light touch here and there—there's always an article or two to engage the reader. While CRYPTOLOG was originally intended to provide a forum for the informal exchange of information by the DDO technical cadres, it has gone well beyond that. Vigorous exchanges have taken place in its pages that have shed as much light as heat, evidence of commitment and concern.

Along with Virginia, I look forward to a still brighter future: publishing more issues, covering more topics, enticing new authors to write. We intend to continue CRYPTOLOG's tradition of challenge and openness. But there's a catch: you are not only the readers, but also the writers. The future of CRYPTOLOG truly depends on you, the readers, to provide the copy, to write the letters, to add that one more piece of information.

I exhort you to lay fingers on keyboards, and put in writing the concerns you talk about around the coffee pot. Don't just talk about them, write them up! You need not limit the scope of your technical exchange to your immediate coworkers. Put your ideas and experiences in CRYPTOLOG and share them with fellow professionals, some of whom you may never have met—some older, some younger. This is ultimately the value of CRYPTOLOG. You can enhance its value by writing for it.

THE GREAT CONVERSATION



Interagency OPSEC Support Staff

This is an extract of a talk delivered at the first National OPSEC Conference, the Maritime Institute, Baltimore, Maryland, April 1990. A complete trascript was published in the Operations Security Monograph Series, under the title, The Great Conversation, *April, 1991.*

The concept that we call "operations security," or OPSEC, reflects ideas and motivations that are as old as the history of human conflict, but as an organized program based on a more or less defined methodology it is a little over two decades old. Its history has not yet been written, and it is still more of an oral tradition than anything else. I've had the opportunity to observe and take part in some of the events that transpired in the two decades that brought the idea from the battlefields of Southeast Asia to the Oval Office. In my short address I'll briefly describe how this concept emerged, how the idea was disseminated beyond Southeast Asia, and how it ultimately was transformed into a national program. While it may not be a children's bedtime story, it's a pretty good yarn.

Three Sundays in the 20th Century

Let me set the stage by telling you what happened on three Sundays in the twentieth century. There is a common thread that ties together the events that occurred on these Sundays, and our being here today is particularly tied to the most recent of these Sundays. The dates of the three Sundays are June 28, 1914; December 7, 1941; and February 6, 1965. Sunday, December 7, 1941, "a day that will live in infamy," was, of course, the date of the Japanese attack on Pearl Harbor and the first day of America's combat involvement in the Second World War. What happened then in 1941 echoed what happened in 1914. No, it wasn't the date when the guns started firing on the Western Front but, in retrospect, they were the first shots of the carnage called World War I. On that Sunday in 1914 in Sarajevo a young Serbian nationalist, Gavrilo Princip, fired two shots and killed the heir to the Austro-Hungarian throne, Archduke Franz Ferdinand, and his wife Sophie. The response of the Austro-Hungarian Government to the assassination led to a train of events that soon engulfed all of Europe. It was the opening bell for round one of a three-round conflict that has consumed most of the twentieth century: World War I, World War II, and the Cold War.

Sunday, the 6th of February 1965 is an outgrowth of the Cold War. And while it is not imbedded in our nation's memory like December 7, 1941, it is no less significant because it was on that date that the longest war in America's history can be said to have begun. In the early morning hours at a town called Pleiku, some two hundred miles north of Saigon, a platoon of Viet Cong troops made a surprise attack on American military personnel at the airfield there. Eight Americans were

killed and 119 wounded. This was a direct assault on Americans whose role in Vietnam up to that time had been purely advisory. This was not the first attack upon American personnel and equipment in the south, but it was the first attack that resulted in a continuing American military response. (I use the word "continuing" to distinguish our response at this time from the "quid pro quo" response to the Gulf of Tonkin incident six months earlier.) With President Johnson's approval, a campaign of fighter-bomber strikes against military targets in the North Vietnam was begun. Known as "Rolling Thunder," these air operations played a unique role in the emergence of OPSEC as a concept and as a program.

The first Rolling Thunder mission was flown on February 11, 1965 four days after the attack at Pleiku and one day after another bloody attack on American personnel at Qui Nhon. Our war had begun, and I do wonder whether we would all be here today if Gavrilo Princip had missed on that Sunday in 1914. We can only speculate idly about this.

As the Rolling Thunder missions continued to be flown in the weeks and months that followed that Sunday in early 1965, they were accompanied by normal military concern over retaining the element of surprise. This concern gave rise to a Joint Chiefs of Staff-initiated undertaking to identify any actual or possible sources that the enemy might exploit to derive forewarning or foreknowledge of our intentions. Such identification could provide a rational basis for the development of countermeasures. This undertaking, of course, was the genesis of OPSEC and began a train of events which has finally brought all of us here today.

Origins of the Term "Operations Security"

Now let me jump ahead in time some two years to the spring of 1967 and shift the scene to the bar in the Officers' Club at Camp H.M. Smith, Hawaii, the site of the Headquarters of Admiral U.S. Grant Sharp, Commander-in-Chief, Pacific (CINCPAC). Four of my associates were exercising the dice cup and discussing subjects that seize men's minds at such times. They also addressed the question, "What are we going to call ourselves?" They were, in fact, continuing an extended discussion about naming a new branch to which they would be assigned that was going to be established within the Operations Directorate of the CINCPAC staff. "Purple Dragon," the name that had thus far been applied to their activities, was considered inappropriate for a staff element. Respectable functional titles were the rule of the day. "Purple Dragon," in fact, was a rather exotic, unclassified nickname from a Joint Chiefs of Staff repertoire that was applied to the one-time "survey" that they and a number of other persons had just completed. The Purple Dragon survey addressed retaining the element of surprise vis-a-vis the Rolling Thunder missions (which provides our linkage to the events on that Sunday in 1965 of which I've already spoken), and two other air operations that were subsequently begun in southeast Asia, the B-52 "Arc Light" operations, and unmanned drone operations.

What do you call a new organization whose mission would be to continue to perform Purple Dragon-type surveys, i.e. an activity to identify actual or probable sources of enemy advance knowledge of our intentions? There was no problem in agreeing on the inclusion of the term "operations," since military operations was what it was all about. But then what would follow? The most appropriate candidates were "Operations Analysis," "Operations Assessment," and "Operations Effectiveness." Each had its merits. The Purple Dragon methodology was analytic; and yes, it did involve an assessment to determine the extent to which we were denying critical information to the enemy; and, ultimately, it was concerned with improving our operational effectiveness.

But neither "Operations Analysis" nor "Operations Assessment" sounded unique among the welter of titles within the Department of Defense, and "Operations Effectiveness" (which, to a man, we considered the most accurate term) just didn't seem to grab one's imagination. But worse than that, the language of the Department of Defense is not English. It is a strange mixture

of familiar sounds interspersed with other sounds that are called acronyms. And was the Department of Defense ready for acronyms that would be derived from Operations Assessment or Operations Analysis? Thus these terms were rejected. What about "Operations Security?" It makes a nifty acronym that can be stated clearly by even the most fuzzy-tongued speaker. But where did "security" come from? Was this choice due to a profound and searching intellectual discourse on the part of the conversants at the bar in the Camp H.M. Smith Officers' Club? Hardly. Between rolls of the dice for the next round of drinks, the sole civilian in the crew thought it would be a neat idea if the name of his employer was included in the title of this new branch on the CINCPAC Staff. His employer was the National Security Agency, and the middle name of his employer followed nicely after "operations." Indeed, it did make a rather good acronym, but [redacted] was motivated less by the appropriateness of the title than by the fact that inclusion of "security" would increase the chance that he, a communications security specialist, would be assigned to it. At some time in the foggy discourse, the prospective chief of the new branch, Air Force Colonel Jim Chance, grunted approvingly.

P.L. 86-36

And thus it came to pass that "Operations Security" was born at the bar in a saloon in Hawaii. As for [redacted] he was right. Characterizing this branch as a "security" organization clinched his assignment to it.

For myself, [redacted] and the rest of the men who were assigned to this new branch and who applied the OPSEC survey concept to combat operations in Southeast Asia, the term "security" was a bit wide of the mark. Our thought processes were geared to terms such as "effectiveness," "surprise," "indicators," "foreknowledge," and "forewarning," and most of the time we used "Purple Dragon" in lieu of "Operations Security." The cover for the regular OPSEC reports that we produced, for example, was emblazoned with a rather striking illustration of a dragon and the words "Purple Dragon." But in retrospect, opting for "Operations Security" was a good decision for reasons that were not foreseen by the stalwart few.

In my opinion, OPSEC by any other name would not have lasted beyond the Vietnam War. We live in a world of symbols, "sound bites," and executive summaries, and the implications of a title can have as great an impact as lengthy, conceptual discourses. The term itself, "Operations Security," has probably had as much, if not more, of an impact than any number of written and verbal explanations of the concept it entitles. It has both a built-in righteousness (who in their right mind could be against such a thing?), that it is something different from plain old "security," and an intriguing absence of complete clarity (I think I know what you mean, but you'd better explain). I doubt whether "Operations Assessment," for example, would have seized the imagination of civilian executive-level decision makers during the years in which OPSEC was transformed into a national program.

And so in the course of a rambling discussion in April 1967, under the most casual of circumstances, a proper noun was agreed upon. It is at best a minor footnote to an episode of the Vietnam War, let alone the cataclysmic events of this century. But it has had an effect upon all of us who are here today. Ironically, a few steps from the bar in the Camp H.M. Smith Officers' Club is the veranda from which you can gaze upon Pearl Harbor in the distance, and if you listen closely, you can almost hear the echoes of the infamous Sunday in 1941.

Disseminating the Idea: the Vietnam Years

The formal establishment of the CINCPAC OPSEC branch occurred in June 1967. For the next five years this small organization conducted some sixty or so OPSEC surveys. Most of these were of combat operations in Southeast Asia, but a number of them addressed operations elsewhere that continue to this day. During the years 1967 through 1972, OPSEC was a concept that was primarily applied by the 17 members of the CINCPAC OPSEC branch (who, not surprisingly, spent most of their time in Southeast Asia), a few officers assigned to the

Military Assistance Command in Vietnam, and a sprinkling of persons assigned to some other major commands. The major focus was, of course, on combat operations.

Throughout the war years, the CINCPAC OPSEC branch distributed a series of "Purple Dragon" reports which described the surveys, their findings, and recommendations. To the credit of the CINCPAC himself, these reports were not subject to the normal staffing process. They were essentially distributed as we wrote them. Although classified, they contributed to the dissemination of the OPSEC concept. In addition, representatives of the branch regularly briefed the Joint Chiefs and other high-ranking military and civilian commanders and managers in the Washington area. We did this two to four times per year. In my own opinion, the regular briefings and across-the-table conversations we had with the Joint Chiefs themselves sustained that vital ingredient of program success: command emphasis. I had a feeling that they looked upon us as a source of information that was unfiltered, unfettered, and unaltered by the normal staffing process.

The first formal effort to disseminate the OPSEC concept beyond Southeast Asia and the Pacific command occurred in 1968. Colonel Jim Chance, the first Chief of the CINPAC OPSEC branch, was subsequently assigned to a newly created OPSEC billet within the Operations Directorate of the Joint Chiefs of Staff. Through his efforts and and the efforts of others, the first Worldwide OPSEC Conference was held at Arlington Hall in the Washington DC area in April 1968, less than a year after the establishment of the CINCPAC OPSEC branch. Attended by military and civilian representatives from throughout the Department of Defense and one or two other agencies, the OPSEC concept was introduced to a broad spectrum of representatives.

At this conference one of my fellow Navy officers, Lt. Commander Bob Johnson, delivered a briefing on OPSEC methodology. In a few words he expressed what I believe is a fundamental precept of OPSEC: "We put ourselves in the position of the adversary and study our operations step by step, from conception through execution to completion and beyond." To this I would add, that whenever possible we correlated this chronological, step-by-step information about our operations with whatever we knew or could reasonably postulate about what the enemy was concurrently doing that could reduce the effectiveness of our operations. Such correlation provided unique insights and a means to isolate what we referred to as "indicators."

Post-Vietnam Loss of Focus

After the U.S. combat role in Vietnam ended in the spring of 1973, the CINCPAC OPSEC branch dwindled in size, eventually being reduced to a single officer and an NSA representative. OPSEC had entered the doldrums. Without a war, OPSEC had lost its focus. But the OPSEC process that had been devised was actually applicable to any competitive or adversarial situation, whether in peace or war, or in the civil or commercial environment. Now it had to be applied, interpreted, and explained in ways that would make this evident. It had to be divorced from the notion that OPSEC was an exclusively Vietnam War activity. What was originally conceived as a pragmatic response to relatively short-term combat operations in which the measures of effectiveness were generally apparent, e.g., loss rates, bomb damage assessments, now had to be adapted to longer term, non-combat operations in which the measures of effectiveness were not readily apparent. At the same time, the omnipresent problem arising from its name, that OPSEC was nothing more than a conglomeration of security programs, had to be overcome. Not without difficulty this is what was accomplished in the post-Vietnam years of the 1970s. The main vehicles of this accomplishment, I believe were:

- Joint Chiefs of Staff support and establishment of programs in the military services;
- adoption of the OPSEC process to peacetime, non-military activities by NSA;
- the "Great Conversation."

Role of the Joint Chiefs of Staff

After the first JCS-sponsored OPSEC Conference in 1968, some six years passed before another

such conference. But beginning in 1974 the JCS presented a series of annual two- and three-day "Worldwide OPSEC Conferences." With the exception of two years, a conference was held each year through 1988.

The JCS conferences, attended by up to one hundred representatives from throughout the government, were valuable forums in which ideas were exchanged and the challenge of adapting a combat-oriented concept to the circumstances of a peacetime environment addressed. At the same time in the latter 1970s OPSEC programs, at least in name, were being established within the military service and the Unified and Specified Commands, accompanied by implementing directives and regulations. Although there was no unanimity of agreement as to what OPSEC was or ought to be, and even though the resources dedicated to OPSEC were usually meager, the important thing was that OPSEC was afforded enough emphasis to keep the idea alive. By the end of the decade the military services and the Unified and Specified Commands were conducting their own OPSEC surveys.

Role of NSA: The Great Conversation

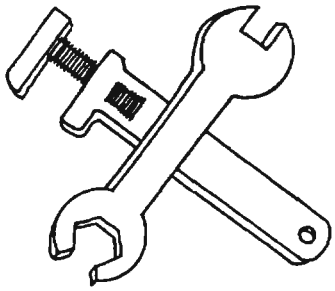
In addition to the JCS Conferences and military programs, the corporate knowledge from the OPSEC experience in Vietnam was being assembled at the National Security Agency, more by accident than design. A few persons who had applied and developed the concept in Southeast Asia were already working for or were hired by the Agency in the early 1970s. Further, NSA continued to fill, without a break, its single billet in the CINCPAC OPSEC branch and became its corporate memory. Through these individuals NSA became the purveyor of the original concept and vital element in adapting it to peacetime military and non-military operations and activities. In due course this was conveyed to other departments and agencies. But this was not without difficulty, since there was the perennial problem arising from the name "operations security." Some chose to emphasize "operations," while others chose to emphasize "security." A lot depended on the interpreter's background and area of interest. However, the NSA experience, in turn, was informally conveyed to others in the Washington community and contributed to a phenomenon through which ideas rise and fall. I allude to the phenomenon which is often blithely termed the "cocktail circuit," but which I would rather, and believe more appropriately, refer to as a "great conversation."

CONCLUSION

We're here today as a result of an initiative by the Interagency OPSEC Support Staff. This staff, in turn, was established as a result of national policy set forth in January 1988. But the policy directive was the result of events and circumstances which transpired since the advent of "Purple Dragon" almost a quarter of a century ago and the emergence of what I have characterized as a "great conversation" about OPSEC. All of us are participants in this conversation during and after this conference. What I've briefly covered here can hopefully add an element of historical perspective to this conversation.

In conclusion I would add that the story of OPSEC is a story about the durability of a good idea that was, at one time, nothing more than a pragmatic response to circumstances relating to combat operations. But in retrospect, the concept that we call "operations security" did not survive and become a national program because it has a catchy acronym, or because it was skillfully proselytized, or because of the challenges that face us in the Information Age, or for any number of other reasons; rather, I would submit, OPSEC lasted beyond the Vietnam War and became a national program because of two primary reasons: one, very simply, it's a good idea. But that's not enough in a world of competing ideas and interests. And this leads to the second reason. I've alluded to it throughout my talk without actually spelling it out. OPSEC endured and became a national program because it has had top-down support. In whatever agency or department of the government, it has become a viable program only when it has had top management backing, and when this is lacking it has not succeeded. If there are any lessons that are to be learned from the history of OPSEC, this is certainly one of them.

OPSEC as a Management Tool



P.L. 86-36

[redacted] A04

(U) Operations Security (OPSEC) is not a security program intended to protect **only** classified information. It really is a business management tool for **controlling** systems and information, classified or not, that expose vital Agency operations to unauthorized persons.

~~(FOUO)~~ Nothing about OPSEC procedures themselves is unique to SIGINT, intelligence in general, or even Government operations. Of course, the secrets NSA protects, and some of the means used to protect them, are specifically SIGINT-oriented, but that's because SIGINT is the business NSA is managing. The same principles apply whether the secrets being protected are:

- (U) Plans for a surprise birthday party;
- (U) Christmas presents for a child;
- (U) An impending acquisition, new product line, or bankruptcy by a company;
- (U) A country's plans to go to war, and fighting the war;
- ~~(FOUO)~~ Intelligence sources, methods, and results.

~~(FOUO)~~ There are many ways to use OPSEC, and there are many ways to penetrate it. Spouses infer plans for surprise parties from demands to be home by a certain time. Children learn where to look for hidden presents. Civic associations use various means to ferret out and contest the plans of developers. Drug runners monitor law enforcement operations to evade the law. All of these are OPSEC penetrations, just as careless management of SIGINT can make possible the penetration of NSA secrets.

(U) The essence of OPSEC is expressed in the Native American prayer, "Oh Great Spirit, before I criticize my neighbor, let me walk a mile in his moccasins." OPSEC is about managers placing themselves in the moccasins of others. It's about using the perspective of the person one wants to keep uninformed to identify ways that that person can use to help gain information the manager wishes to keep secret. And it's about taking cost-effective countermeasures to defeat such efforts.

~~(FOUO)~~ This challenge goes beyond the traditional security procedures so respected at NSA. In our business, we're used to protecting "classified" information. But people desiring that information don't care whether we consider information "classified"; they consider only whether it might be useful to them. Even the new Government category "unclassified but sensitive" doesn't completely encompass what these people might find useful for their purposes.

~~(FOUO)~~ For OPSEC purposes, managers ought to consider the terms "no need to know" and "unauthorized person" interchangeable. Sometimes people think of only "hostile intelligence services" or terrorists as adversaries to whom we must deny our secrets. NSA managers also should think of the following to be denied access, in approximately descending order of benignity and increasing order of access to sensitive data and methods:

- ~~(FOUO)~~ People who for some reason want to prevent the Government from doing intelligence work;
- (U) News media and authors seeking an exclusive story;

• ~~(C-CCO)~~ Intelligence users (who often insist upon information about sources and methods which they don't need);

• ~~(FOUO)~~ Foreign collaborating services (especially Third Parties) who aren't participating in the specific project; or even

• ~~(FOUO)~~ NSA Green Badgers without a need to know (for example, with compartmented projects);

~~(FOUO)~~ The OPSEC process works best as a project-specific, cost-risk analysis integral to management thinking. It needs to be project-specific, because each project has its own operational and security characteristics. It begins with defining as specifically as possible:

• ~~(FOUO)~~ What "core secrets" must be protected if a project is to meet its mission;

• ~~(FOUO)~~ Who the "adversaries" are for that project (that is, who outside the project might be trying to learn its secrets);

• ~~(FOUO)~~ What capabilities these adversaries have to gain access to and use the information or equipment to be protected;

• ~~(FOUO)~~ What there is about the management of the project that makes it vulnerable to those capabilities; and

• ~~(FOUO)~~ What, if anything, can be done to reduce those vulnerabilities.

(U) Managers use information like this to decide how to deal with risks. Sometimes, they decide that eliminating a specific vulnerability is impossible without cancelling the project entirely. Sometimes they decide that certain vulnerabilities are too low a risk to justify the cost and effort to eliminate them. Sometimes they decide that steps to remove a risk would have the opposite effect of calling attention to it, and the best thing to do is nothing. And sometimes they make changes that remove the vulnerability, or at least reduce it to acceptable levels of risk.

~~(FOUO)~~ Project managers sometimes want to consult outside advisors to help them identify system vulnerabilities and threats. NSA has in place a network of OPSEC coordinators to provide help of this kind. This is when an OPSEC Survey is a useful tool. A team is formed of people knowledgeable in the technology or kind of operation to be studied, but not involved in managing that project. The team applies its experience to study the project the way the adversary would study it, and report to the project's managers the weaknesses they find, as well as logical ways these weaknesses can be removed. (They become, in effect, a "Red Team," to compare their findings with those of the "Blue Team" comprising the project management.) The survey team is duty-bound to treat the study results as the property of the regular management team, just as a contractor would do if hired commercially to do the survey.

(U) Like all management processes, OPSEC requires follow-through. An ongoing program has a continual stream of management decisions. Some degree of cost-risk consideration should be a factor in each of these decisions. OPSEC is at its functional best when this happens.

DIRECTIVES

(U) In January, 1988, President Reagan signed National Security Decision Directive (NSDD) 298, which designated NSA as the executive agency for providing Government-wide training in OPSEC. In response, NSA formed a Directorate of OPSEC (D2) and also the Interagency OPSEC Support Staff (IOSS), which has offices in Greenbelt, MD. The IOSS has staff officers from several government agencies. It provides a range of OPSEC awareness and assistance programs, including publication of a series of monographs and publications. Those who want to know more about including OPSEC in their management thinking are urged to get copies of these monographs from their OPSEC coordinators, the OPSEC Directorate, or the IOSS.

~~(FOUO)~~ An NSACSS Directive (No. 120-01) provides OPSEC procedures and instructions. NSACSS Circular 25-5 requires that Systems Coordination Papers (SCPs) and Program Baseline Summaries (PBSs) include discussion of OPSEC planning for new NSA programs.

TRAINING

~~(FOUO)~~ The National Cryptologic School's Management Faculty (E9) offers a one-day orientation class (OP-200) in OPSEC. There also are OPSEC modules in some other Cryptology courses. The faculty there welcomes critiques of these courses and suggestions for others.

SOME EXAMPLES OF OPSEC VULNERABILITIES

(U) *The launch profile of spacecraft.* Media reporters often deduce from these profiles when intelligence satellites are launched. This is an OPSEC vulnerability that cannot be removed and at the same time, ensure that the the satellite is put into the right orbit.

(U) *The azimuth and elevation of a satellite antenna.* An alert person armed with a Boy Scout compass can measure these and learn toward what geo-stationary satellite the antenna is pointed.

P.L. 86-36

(U) *Parking lot analysis.* What cars are parked in the reserved spaces of senior executives can reveal which executives are away from the office. (Some executives blur this by letting their secretaries use their spaces when the executive will be absent.)

[redacted]

EO 1.4.(c)

[redacted]

[redacted]

[redacted]

(U) It should be clear that good OPSEC is not some elaborate or revolutionary new management concept. It is merely an orderly and common-sense way to keep one step ahead of opponents in managing the business of SIGINT.

BOOKBREAKERS FORUM

on

MACHINE AIDS

If you are working on codes, programming for codes, or managing a code problem, join the Forum and exchange methods and techniques with others doing the same type of work.

Write your Name, Organization, and Building on a piece of paper and send it to the Chairman:

[redacted]

2509
North.

P.L. 86-36

Please re-register even if you are an old hand, for the reorganization has played havoc with the mailing list.

~~FOUO~~

[redacted] E34

WHERE WAS THE BOGEYMAN?

An Analysis of the Response of Islamic Fundamentalist Groups to the Persian Gulf Crisis

(U) Who could forget those chilling scenes in late 1979 when Iranian "students" took over the U.S. Embassy in Tehran? Hordes of Muslims marched in the streets chanting "Death to the Great Satan", burned effigies of President Carter and Uncle Sam and exhorted fellow Muslims to rise up against the West. These pictures, repeated over and over throughout the entire Iranian hostage crisis, were burned into the minds of Americans and other Westerners. For years after the hostage crisis, the foreign policy of the United States and other Western countries on the Middle East seemed to be based upon the premise that some new situation or crisis could again ignite the fundamentalists' fervor and unleash a "bogeyman"--mobs of sword-wielding Muslims sweeping down on the non-believers as punishment for their transgressions against Islam.

~~(TSC)~~ Just prior to the invasion of Kuwait in mid-July 1990, [redacted] in Iraq Saddam Husayn called for Kuwait and other Gulf oil-producing countries to relent on their over-production of oil quotas or face Iraqi retribution. That speech set in motion events that tested the resolve of not only the Secretariat but of all Islamic Fundamentalists throughout the Middle East.

(U) Saddam Husayn's occupation of Kuwait in the summer of 1990 precipitated what many thought would be the event that would unleash the fury of Islamic fundamentalism. Shortly after the occupation, he issued a call to all Muslims for Jihad (Holy War) against the United States and other Western countries who had come to the aid of Saudi Arabia. But according to Islamic law, Husayn had no legal basis for his call for Jihad. His use of the term Jihad was probably intended to bolster the morale of the Iraqi people in general and the Iraqi military in particular. The fact that he could not legally call for Jihad suggests that Husayn's strategy may have been to play on the fears of the U.S. and other Western countries.

(U) Islamic law (Shari'a) sets out the conditions under which Jihad can be invoked. As law, the Shari'a is subject to interpretation and the various sects of Islam have each chosen to define Jihad in their own way. The largest sect of Islam, the Sunni, has adopted the most conservative interpretation, in which Jihad includes both temporal and spiritual efforts to defend Islam. In fact, the Sunnis have identified four types of Jihad: of the heart, the tongue, the pen and the sword. The first three of these address challenges to Islamic values, including a personal moral struggle of the soul. The fourth refers to a challenge from a non-Muslim source, such as that posed by Operation Desert Storm. The Shi'ia sect of Islam, the most radical, tends to have a more militant interpretation of Jihad. Their concept of Jihad

embraces the idea of martyrdom. The Shi'ias have even extended their definition of Jihad to include the Sunnis, whom they regard as heretics who must be brought back to Islam.

(U) Technically in today's Islamic world, no single Muslim leader can declare Jihad. The schism created by the secession struggles after Mohammad's death has, over the many centuries of Islamic history, eroded the legal and religious authority to declare Jihad for all sects of Islam. Islamic jurists agree, however, that Jihad against an enemy threatening the very existence of Islam itself remains a collective obligation of the entire Muslim community.

(U) Saddam hoped, in addition to bolstering the morale at home and among his troops, that his call for Jihad would have an emotional impact among all Arabs and galvanize support among Islamic fundamentalist groups for his struggle against the coalition forces. Indeed, during the early period following the Iraqi occupation of Kuwait, some groups heeded the call, but not in the way that Saddam Husayn had hoped.

~~(TSC)~~ The evidence suggested that these groups were intent on defending the honor of Islam vocally or intellectually rather than taking up a military or terrorist option. Indeed, as the occupation wore on, it was clear that the majority of fundamentalist groups did not really care about Husayn's religious beliefs, but were intent upon their own nationalist goals and attempted to use the Persian Gulf crisis as a front. In general, the Persian Gulf crisis appeared to provide various fundamentalist groups with a perceived legitimate reason to stir up dissent in their own backyards. Diplomatic observers in many countries in the region saw the popular dissent surrounding the crisis as resulting from pressure from local fundamentalist groups upon their governments.

~~(TSC)~~ Arab countries supporting the coalition, especially Egypt and Saudi Arabia, expected fervent reactions from indigenous fundamentalist groups. As it turned out, there were demonstrations and protests, but nowhere close to the number expected or predicted. The Muslim Brotherhood in Egypt staged protests in mid-September and early October 1990, but even these revealed inconsistencies in the fundamentalists' objectives. Several of the demonstrations decried Husayn's annexation of Kuwait as the 19th province of Iraq, but at the same time protested the U.S. and Egyptian involvement in the crisis. It soon became apparent that various Egyptian social and political issues were behind many of these protests, once again indicating that the crisis was being used as a springboard for local fundamentalist objectives. Saudi Arabian fundamentalists, on the other hand, declared their willingness to actively oppose Saddam Husayn and volunteered to defend Saudi Arabia's holy cities of Mecca and Medina against aggression. Morocco, another Arab country that was part of the coalition, was also the scene of some fundamentalist protests; these the local diplomatic observers dismissed as minor, unplanned incidents.

~~(TSC)~~ Elsewhere in North Africa, both Algeria and Tunisia were more overt in their support of Husayn's actions. But even there, the response to the crisis by local fundamentalist groups was not overwhelming. The growing fundamentalist movement in Algeria, the Islamic Salvation Front (FIS), swayed the government to announce its support for Husayn's invasion of Kuwait. But the Algerian government stopped short of supporting Iraq's annexation of Kuwait. This indication of the government's ambivalence in the crisis was attributed to the fact that various political and social groups in the country, including the fundamentalists, were all seen as using the crisis to gain power for themselves. Diplomatic observers even hinted that the FIS, the strongest of the Algerian fundamentalist groups, was using the crisis to cover up its poor performance at home. In

Tunisia, however, the struggle was along more classic lines. The rift within fundamentalist groups appeared to be between the leaders, who leaned toward supporting Kuwait and Saudi Arabia, and the younger members of the groups, who supported Iraq.

~~(TSC)~~ As the birthplace of modern Islamic fundamentalism, Iran might reasonably have been expected to play a leading role throughout the Islamic world with respect to the responses of fundamentalists against Operation Desert Storm. To be sure, Iran played a role, but it could not be characterized as a leading one; it adopted a wait-and-see attitude. This was consistent with Iran's overall policy during the war, which was one of relative neutrality towards both sides in the conflict. Several smaller fundamentalist groups, notably in North Africa and the Sudan, took pains to seek Iranian guidance and advice before publicly responding to the crisis. This was probably an effort by these relatively minor groups to acknowledge Iran's leading position in the fundamentalist world and achieve some measure of credibility in their own countries by being perceived as having Iranian support for their actions. The Maghreb Islamic Movement in North Africa even sought Iran's view on the legality, under Shari'a, of sending volunteers to fight alongside Iraqi forces.

~~(TSC)~~ A more universal fundamentalist response to the situation in the Gulf was noted in Jordan, which might have been expected in view of King Hussein's overt support for Saddam Husayn. Early in the crisis, the Jordanian Muslim Brotherhood attempted, unsuccessfully, to mobilize the support of fundamentalist groups in Egypt, Syria, Iraq, and several other Islamic countries. Muslim Brotherhood members of the Jordanian Parliament were outspoken and vocal in their support for Husayn, taking the view that the larger issue was one of a battle between Islam and the "infidels".

~~(TSC)~~ The regional experts who foresaw that some situation or event would unleash the full fury of Islamic fundamentalism upon the offending foreign power(s) did not find it in Desert Storm, which pitted not only Muslim against "infidel", but also Muslim against Muslim. The predicted fury of the Islamic uprising turned out to be just a handful of localized events that fizzled out with no serious impact, not the all-encompassing force some had predicted.

(U) Does the "bogeyman" exist at all? It's not clear, as there were ambiguous circumstances in Desert Storm that cloud the issue. It was not clearly an infidel versus Muslim affair, and many Muslims recognized the invalidity of Husayn's actions. Were there to be another situation in which the US or other Western power attempted to unilaterally insert itself into the internal affairs of an Arab nation without UN sanction, it could be a different story. Under *shari'a*, this could be interpreted as threatening the very existence of Islam and make it easier for Muslims to act together, and a call for jihad might then be effective.

~~(TSC)~~ The Gulf crisis did not produce a region-wide, cohesive Islamic fundamentalist response. Consistent with the history of politics in the region, fundamentalists and their organizations used the crisis as a springboard for their own particular political or nationalistic agendas. Even Saddam Husayn's call for Jihad failed to coalesce the various personalities or groups.

END NOTE

~~(C)~~ [redacted] provided an excellent treatment of the subject of Jihad in relation to Operation Desert Storm in DIA Defense Intelligence Memorandum DIM 32-91, January 1991.

OGA

There Never Was a Bogeyman

a Reply

Peter D. Molan, P04/SLA

When [redacted] gave me a pre-publication copy of his article, I read it with the sense of satisfaction that one feels when one sees that the views of a respected colleague are in accord with one' own--until I reached the conclusions. Then I was disturbed.

It was clear to me that the whole thrust of Ron's article had been to debunk the threat of a wide-spread rally to Saddam Husayn's call for a *jihâd,* a "Holy War," against America in the run-up to Desert Storm. And yet, Ron's conclusion--despite all the evidence which he himself had mustered to show that the fear had been overblown--was that we must be on the alert to that very danger in the future. I believe that Ron's conclusion plays into the hands of a troubling tendency which is more and more apparent in American thinking.

As *Washington Post* commentator Jim Hoagland noted on 6 February '92, we seem to have "an urge to identify Islam as an inherently anti-democratic force that is America's new global enemy now that the Cold War is over." The manifestations of that urge are rife. The most egregious example I know of appears in an article by *Newsweek's* chief diplomatic correspondent, John Walcott. It dates back to 15 July 1985, but is a common enough, if particularly virulent, statement of the urge:

"Fighting terrorism is not unlike fighting *malaria.* It is not enough to swat the mosquitoes; it is necessary to drain the *swamps* where they breed ... (but) ill-considered or poorly executed attacks on suspected terrorists (in Beirut) may only succeed in replacing today's Republic of Nihilism with something even more dangerous: the Islamic Republic of Lebanon... Preventing such a vulture from hatching should be the goal of the United States..." (my italics).

More recently, Rowland Evans and Robert Novak in a *Post* column of 2 March '92, expressed their fear of a "dangerous fundamentalist *tide*" arising from Iran and sweeping over Central Asia (my italics).

Where does the disgust and loathing of Islam which are manifest in such statements come from? Are they really rooted in, and justified by, the harsh punishments specified by Islamic law for theft, fornication, and apostacy as occasionally applied in three or four countries? I doubt it. Such loathing is generally rooted in fear.

That fear seems to be linked to the dreaded word, jihâd--"Holy War"--itself. The word conjures up images, precisely, of Evans and Novak's "tide"--of religious fanaticism--arising out of Walcott's "swamp"--of some uncontrollable primitivism--to overwhelm all that is progressive and good--us--and then pick over our bones like some "vulture"

But, that fear tells us more about our own subliminal terrors than it does about any real "Islamic threat." That fear reflects the primal, childish dread of the bogeyman and not a rational assessment of risk.

Ron has already pointed out the major arguments as to why a wide-spread coalition of Muslims aligned against Western interests is

unlikely to occur. Let me only add an historical observation: ***there never has been a jihâd!***

Muslim leaders always "call for" "Holy War" against the "infidels" when they are in trouble, of course. Every one who has done so, however, has gotten the same reaction that Saddam Husayn did--a brief flurry of attention in certain Muslim circles and then nothing.

The two most famous calls for jihâd came from Saladin, during his struggle against the Crusaders, and from 'Abdul-Hamid II, during World War I. During the Crusades, the Caliph in Baghdad barely deigned to respond to Saladin's appeals for help. Other Muslim Amirs continued lucrative trading arrangements with the Venetian and Genoese merchants who were supplying the Crusaders, and Sultans concluded treaties with Christian Princes against Saladin whenever it suited their purposes. Saladin did succeed in checking the Crusading enterprise, of course, but that success had nothing to do with "jihâd."

When 'Abdul-Hamid called for a Holy War, the Muslim soldiery of the British colonial armies ignored him. The Arabs of North Africa and the Najd remained quiet, and the Arabs of the Hijâz revolted against him. That Saddam would fare no better than his predecessors was entirely predictable.

Posing the question of how serious Saddam's call for a jihâd might be was not inappropriate at the time, of course, but differences of language, sect, nationality, and local history militate against a generalized Islamic threat to the "West" so strongly as to make any great concern about a jihâd silly. There *is* another, *real* danger, of course.

Hoagland describes that danger in these words: "... America now has the burden, and opportunity, of making complex foreign policy choices instead of replacing one set of blinders with another..." To make those choices, American policy makers will have to receive accurate information, from their analysts, on the realities of a world in which more and more people, Christians, Jews, and Hindus, as well as Muslims--be it noted--seem to be turning to religion as a solution to their problems.

As Hoagland points out, "Replacing blind anti-communism abroad with an equally crude anti-Islamic doctrine would be self-defeating." Blind anti-Islamism will prove to be "self-defeating" for two reasons. As an analyst, I believe that the more important of those two reasons is that such blind fears can only distort our abilities to render accurate analysis.

The second reason is that mindless hostility can only provoke a hostile response from those against whom it is directed. Such hostility will scarcely produce a jihâd, but it will complicate relations. When the American Muslim Louis Farakhan described Judaism as "a gutter religion" and White people as "devils" he was loudly, and properly, condemned for anti-Semitism and racism. How do we expect Muslims to respond to those who characterize their religion as a "dangerous tide" or a "malarial swamp" or a "vulture"? How do we expect them to respond to those who do not condemn such rhetoric and the primitive terrors in which it is rooted?

This is not to say that there can be no criticism of Muslim thought. One may, on the grounds of Islamic history as much as our knowledge of human psychology, condemn as absurd the assertion by 'Abdul-Halim Mahmud, the former Shaykh al-Azhar, that "Application of the *hudûd* punishments is the only cure for the spread of the crime which we see today. Stealing will be ended once and for all if we cut off the hand of one thief." But, both our analysis and our criticism must not, for our own sakes as well as for the sake of our relations with our Muslim neighbors, descend to the realm of the irrational fear and distorted thinking manifest in a grossly exaggerated concern over "jihâd."

Note: **NEW** mailing address for

CRYPTOLOG
P0541
OPS-1

NEW e-mail:
cryptlg @ curator

P.L. 86-36

~~SECRET~~

SANDLOT

[redacted]

Networks

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

P.L. 86-36

[redacted] T336

~~(C)~~ The SANDLOT program was originally envisioned as a more-or-less turnkey analytic support system. [redacted]

Today SANDLOT is not a turnkey system; rather, it is a flexible, modifiable, tailorable system, one that allows users to dynamically select software alternatives according to individual preferences. [redacted]

P.L. 86-36

A Word on Terminology

~~(C)~~ SANDTERM is software that runs in a user's workstation and facilitates connectivity and communication. [redacted]

DOS Compatibility

(U) Although SANDLOT itself is firmly wedded to the Unix operating system, workstation technology and commercial software have evolved to a state where most workstations permit users to freely traverse between the entirely commercial DOS software applications world and the Unix connectivity-oriented environment.

Editors

(U) SANDLOT supports the in-house developed [redacted] which is used in [redacted]

P.L. 86-36

because of its superior performance, the choice is up to the individual analyst.

Database Systems

(U) SANDLOT permits the user to select from among a variety of commercial Unix Database Management Systems such as INGRESS, Sybase, and BRS Search; and also supports the in-house

Electronic Mail

(U) User-friendly electronic mail has transformed the way business is conducted at the Agency.

Desktop Publishing

(U) SANDLOT supports both the INTERLEAF and FRAMEMAKER commercial desktop publishing systems.

Applications

(U) By observing a few simple rules and using shared code libraries, applications developers all over DDO have been able to produce software

There are two substantial benefits to this approach:

- the applications programmer delivers software to the user with the same user interface — the same look and feel — as all his other software;
- he has removed substantial risk as to the portability of his code when new hardware is purchased.

Sharing Resources

(U) With the deployment of large numbers of Local Area Networks (LANs) under the SANDLOT program it has been possible to widely share costly resources such as letter-quality printers and color plotters amongst large user populations.

Software Standards

(U) By adopting the toolkit approach to SANDLOT, significant time and money was saved in the acquisition process. Additionally, customer satisfaction is higher because permitting substantial choice in tool selection and development enhances the customer's feeling of "ownership" of the system. Certain software standards have been most important in achieving this goal:

- Unix, primarily AT&T System V Unix, but with some difficulty SunOS as well;
- X11 — an industry standard, adherence to which provides complete software portability for keyboards and display devices;
- TCP/IP communications protocol, enabling networks to be reliably and quickly developed.

(U) We are enthusiastic about further standards development which might continue to make our job of delivering analytic support easier in the future.

Conclusion

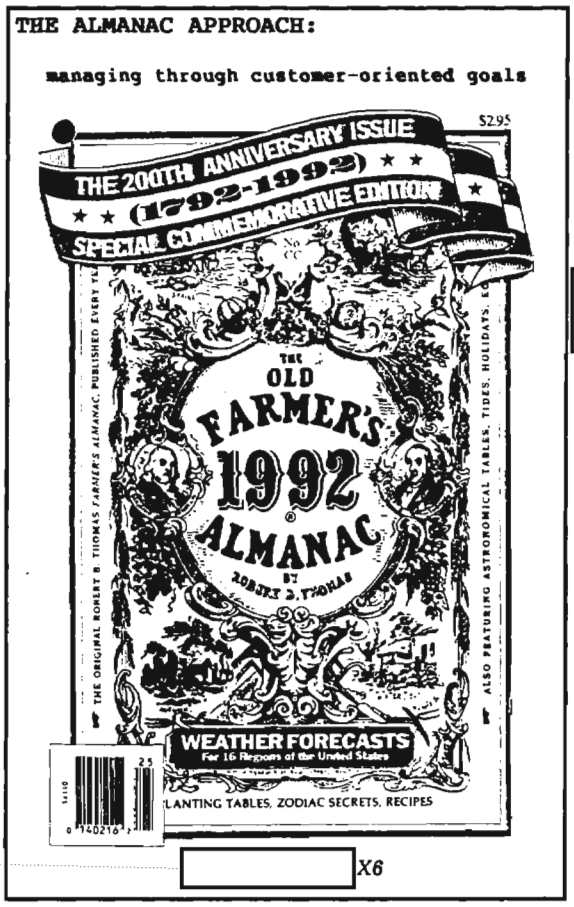
~~(C)~~ Industry-wide software standards, coupled with more and better commercial software are making possible the more rapid development and deployment of significant end-user capability. The SANDLOT program has been able to integrate more commercial software than ever before, while preserving necessary NSA-unique software. This approach has yielded dividends to SANDLOT end users who have the benefits of access to NSA-specific data, yet the manipulation tools of the commercial world.

Note NEW mailing address:

CRYPTOLOG
P0541
Ops-1

and new e-mail address

cryptlg @ curator



P.L. 86-36

Have you ever noticed how traditional resource management tools really don't help you manage your resources? Have you ever noticed how seldom your Mission and Function statement, Resource Allocation Document or Table of Distribution has the information you need?

In Y Group we decided that we needed a management planning approach that is more "manager friendly." The result of our efforts is what we call the **Y Almanac**. We believe it may apply to other organizations as well.

The Almanac enables us to identify where we want the organization to go and helps to ensure that we are putting our resources on our stated priorities. It is a customer-conscious, goal-oriented planning system that recognizes the need for obtainable short-term goals, for job ownership, and for quality performance. The following describes the Almanac Approach and why we develop it.

BACKGROUND

Y Group consists of 3 traditionally structured but unrelated office-level organizations. It is the largest Group within the Information Systems Security Organization, both in the numbers of people assigned and in the diversity of skills needed to meet mission requirements.

P.L. 86-36

Our challenge was to find techniques that allow us to "get (and keep) our arms around" such an organization in terms of its tasks and its effectiveness. While traditional mission and function statements define the individual parts, in our opinion they leave something lacking in regard to the organization as a whole. We needed another approach.

Our efforts led us to develop the Almanac, which is a series of six parts providing the in-depth insights we sought. The Almanac is a "living" approach, in that the documents are regularly reviewed and updated. The six parts are:

Goals, Objectives and Tasks;
Task Matrices;
Manpower Utilization Report;
Financial Plan Matrix; .
Accomplishments Report; and
Demographics Report.

THE GOALS, OBJECTIVES, AND TASKS

The use of goals and objectives seems to come and go in management literature--and it seems to be out of fashion at the moment. Nevertheless, we believe some form of a goal-oriented approach is necessary to ensure that everyone in the organization knows where the organization is heading.

The Goals, Objectives and Tasks concept recognizes that lofty, long term goals seldom are motivating forces. People need to be able to work towards something that is obtainable within a reasonable period of time to feel pride in accomplishment, rather than frustration in never getting to the end of a very long journey. At the same time, the organization needs to

reach for things just beyond the immediate or it will become very short-sighted and focus only on the near term.

Our solution is to layer our goals into three levels. The **Goals** are the long term items for which we expect to strive for the foreseeable future. Supporting each Goal are one or more **Objectives**, which are more readily achievable in a reasonable period, though relatively long-term and general in nature. The Goals and Objectives provide a clear picture of the direction in which the organization is moving.

The merger of the organization's long term goals and mid-term objectives with short-term achievable ones is in the **Tasks**. As each Goal has supporting Objectives, each Objective has subordinate supporting Tasks. Each Task is a short term, achievable job, somewhat broadly stated but specific enough that managers and those involved in the Task can clearly understand the boundaries.

The principle of job ownership is task management. Each Task is assigned a Task Manager who is responsible for seeing that the Task is accomplished. We decided that as a general rule, Task Managers should be no higher than division level, and preferably, we push the responsibility down into the organization as far as practical.

In our case, we identified 14 Goals which cover the day-to-day requirements with room for the "stretchy, reach for the stars" items as well. These 14 Goals have over 35 supporting Objectives, which in turn envelope over 170 Tasks. No one is expected to know all of the Goals, Objectives and Tasks. Senior managers know the 14 Goals, and know well those against which they have resources. Every employee should know the Task or Tasks on which he or she is working, and the Objective(s) and Goal those Tasks(s) support. The entire set of Goals, Objectives and Tasks is available to every employee who wishes to know the direction in which the organization is heading.

We looked to the big picture when we considered how to organize the Goals, Objectives, and Tasks for publication. In any organization the work can be categorized into three basic **Activities:** Customer Support; Internal Operations; and Investment in the Future.

- **Customer Support:** All organizations make products for or provide services to customers, some external to the overall organization (**Support to External Customers**), some within the organization (**Support to the ISSO**).

- **Internal Operations:** Work done for the organization itself. This included senior management,clerical support and administrative staffs. We also placed our engineering support here--the work that keeps the production lines going.

- **Investments in the Future:** Successful organizations have to spend some effort to develop new processes, new equipments, or new services in order to remain competitive and successful.

We examined our Goals, Objectives and Tasks and matched them against the activities without regard to the organizational unit in which the work was to be done. This is the point at which we clearly leave the traditional mission and function approach to organization work, for we are primarily interested in the total organizational effort. Some work fits into a single organizational sub-unit, other crosses organizational lines. Key generation, for example, is done in one division in one Office. Quality control, on the other hand, uses manpower in several divisions in each Office.

By arranging the Goals, Objectives and Tasks in their appropriate activity category, we have a clear road map of where the organization is going. To keep the Goals, Objectives and Tasks up to date, they are revised semi-annually. The process begins with the subordinate Y organizations, which recommend changes or additions and deletions. These are forwarded up the chain of command, and are consolidated at the Group level. The draft revision is then re-coordinated with the Y Office Chiefs and published after final approval by the Chief, Y.

THE TASK MATRICES

We demonstrate our commitment to the concept of **job ownership** through the appointment of Task Managers. Each Task Manager completes a Task Matrix, an eight-column document that:

- States the what, where, how, why, for whom and by whom of the Task, to include the quality objective;
- Identifies the resources required to do the Task, and
- Identifies the standards by which success in achieving the Task, to include the quality objective, is measured.
- Notes expected changes in the Task;
- Identifies the resouces required to meet the expected change;
- Defines the delta between what is required today and the expected future change;
- Identifies any issues involved in the new requirements; and
- Identifies the standards by which success in achieving the delta will be measured.

Task Managers brief senior management periodically on their Tasks. We select about 10 Tasks each month to be discussed informally. The Task Matrices achieve multiple management objectives:

- They force local management to think about and commit to writing what they are doing and how they measure success. (Our emphasis on measurement happily coincides with that given under the Total Quality Management philosophy to which the DoD is committed.) For most tasks local managers must formally look at least two years ahead and address the issues. We have found that this aspect has been very beneficial to the Task Manager--some have admitted that in preparing the matrices they looked down the road for the first time.
- They provide an avenue for persons involved in the detail work of the Group for discussions with senior management.

CUSTOMER SUPPORT	ISSO SUPPORT
Goal 1 Goal 2 Goal 3 Goal 4 Goal 5	Goal 6 Goal 7 Goal 8 Goal 9 Goal 10 Goal 11
INVESTMENT IN FUTURE	**INTERNAL OPS**
Goal 12	Goal 13 Goal 14

- During the briefings they offer opportunities for senior managers to observe more directly the capabilities of employees at every level.

THE MANPOWER UTILIZATION REPORT

We also needed a means to provide a good visual presentation of how we employ manpower on the Goals, Objectives, and Tasks. The semi-annual Manpower Utilization Report tells us where our manpower resources are.

It uses a standardized format. For each Goal, the information on the first page:

- identifies the Activity supported at the top of the page;
- provides a Goal overview, stating how many man-years of effort are required;
- lists Objectives in keyword, bullet format;
- identifies pertinent facts the reader should know;
- and states some additional resources comments such as use of overtime or shift work.

When appropriate, the overview page also contains a line graph or bar chart depicting the anticipated future requirements.

We chose to identify separately the management and support overhead involved with these major functions. The Management and Clerical lines are listed under Internal Operations.

Objectives with large numbers--usually 15 or more--of man-years are split out in "break out"

KEY MATERIAL PRODUCTION (Goal)

Objective	Man-Years
Production Requirements	xx
Key Generation	xx
Paper Key Production	xx
Special Key Production	xx
Electronic Key Production	xx
	--
Clerical	x
Management	x

Selected Tasks	Production Facts
* aaaaaaaaa	* zzzzzzzzzzzzz
* bbbbbbbbb	* yyyyyyyyyyyy
* ccccc	* xxxxxxxx

Resources Comments	Forecast
* xxx hour overtime * 2 shift operation	

pages placed immediately behind the overview page. The Activity support is identified in the upper left corner, and the Goal and Objective involved are shown in the upper right corner. For the remainder, the same basic format of the overview page is followed, with the focus on the man-years required for the component parts displayed in a pie chart. For example, a break-out page on the Paper Key production Objective contains a pie chart reflecting the man years if effort involved in Design, Production Control, Typesetting, Photo Lithography, and Press/Bindery operations. The Tasks, Production Facts, and Resources Comments boxes contain specific information about paper key production.

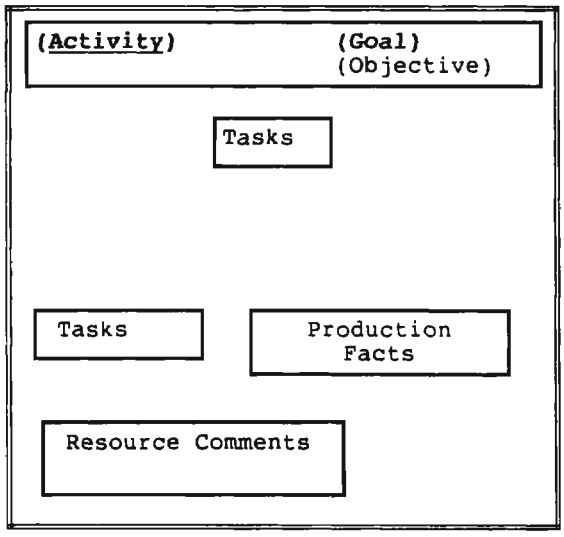
The advantage of this concept is that it tells senior managers exactly what the manpower costs of a function actually are. We found that the traditional TD and RAD approach just doesn't give the whole picture.

THE FINANCIAL PLAN MATRIX

In this part of our Almanac, we look at dollar resources applied to the Goals, Objectives and Tasks. Each line item is matched against the Task which it supports. Thus, we can identify how many dollars we are allocating to each Task, each Objective and each Goal. By combining this Report with the Manpower Utilization Report, we have a complete picture of where we are putting all of our resources.

As stated earlier, our Almanac is a living approach, one that changes and grows as required. An example of one element of the Almanac that has changed considerably is the Financial Plan Matrix. The Matrix, maintained on a PC using LOTUS 1-2-3 software, reflected only the information indicated above. After the first Matrix was published, we added a few columns and some calculations, and now use it as a summary sheet for the entire concept. The Matrix is shown on the top of the next page.

The dollars programmed for each line item are identified by Budget Code and totaled under the Task Column. The man-years of effort for each Task is also shown. In the Objective column, the sum of the dollars programmed for the various Tasks under the Objective are totaled, and the percentage that figure represents for the total dollars programmed for the Objective is shown (% 0). Also, the total man years of effort is shown, both for "line" (n(1)) and for management, clerical and staff (n(a).) The Goal column similarly reflects the total dollars programmed for the Goal, the percentage of the total FINPLAN those dollars represent (% FP),



Goal	Objective	Task	Budget Code	Dollars	Man Years	Task Manager
Aaaaa	Wwwwwww	Ccc	Gxxx	$$	nn	Name
$$$$	$$$	$$				
% FP	% 0					
		Ddd	Nxxx	$$	n	Name
n(1)	N(1)	$$	Lxxx	$$		

and the man-years of effort for the Goal. The Task Manager column is self-explanatory.

THE ACCOMPLISHMENTS REPORT

The Y Accomplishments Report is our annual publication that highlights examples of important things that we have done during the previous Fiscal Year. It follows the format of our Goals, Objectives and Tasks concept, with each accomplishment identified as to the Task, Objective and Goal which it supports. Each page, in key word or bullet format, identifies the Activity, Goal and Objective(s) under which the reported Tasks fall. A sample of a page is shown below.

THE DEMOGRAPHICS REPORT

The Demographics Report, published annually, provides a typical "people facts" summary--facts about grades, educational levels, promotions and awards data, etc.

SUMMARY

The Goals, Objectives and Tasks is the keystone of the Almanac concept. It tells us where we intend to go and how we intend to get there. The complimentary Task Matrices, FINPLAN matrices and Manpower Utilization Report provide senior management the long sought ability to get our arms around the entire organization and plan with more confidence than ever before. Our Almanac approach has proven itself to be a valuable planning management tool over the past two years. It is flexible, and can incorporate new ideas without having to rebuild the concept.

It works.

CUSTOMER SUPPORT **KEY MATERIAL PRODUCTION**

Generate & produce keying material

Selected Tasks	Selected Accomplishments
Paper key & publications	Saved over $xxx,xxx over the base year through the paper waste reduction program.
Sealed systems, tapes, and cards	Produced over xxx,xxx sealed systems, which included almost xx,xxx PAL/CS related products.
	Established yet another production record of x.xx million key tapes, up xx.x% over the FY-88 previous record.

~~SECRET~~

Further to THE TEN MOST WANTED

[redacted] *P04*

P.L. 86-36

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

P.L. 86-36

~~(FOUO)~~ I read the article on The Ten Most Wanted in 2nd Issue 1991 with a great deal of pride, I admit, for I, too, am a former manager of the program. But one thing the article did not mention was how the program got started.

~~(S)~~ The program was prompted by the Future SIGINT Capability Study that challenged NSA, and specifically the Office of Search (W3), to ensure the SIGINT system's survival through the year 2000 in the face of exploding technology. One of W3's reponses was to establish at the DO level the DO Ten Most Wanted Systems Program. [redacted] then DDO, approved the idea, and on 5 April 1986 announcements went out everywhere: fieldgrams, booklets, and posters. In addition, W3 sent message to [redacted]

The first manager was [redacted]

~~(C)~~ One point I did want to emphasize is that it is the ***Operations*** Ten Most Wanted Signals Program. W3 is the simply the manager of the program.

(U) Incidentally, you might be interested to know that the illustration shown above was used as a logo for the program.

~~SECRET~~

WL: in memoriam

We regret to report the death of William Lutwiniak, Founding Publisher of CRYPTOLOG. Following is an appreciation by Doris Miller (ret.), Founding Editor of CRYPTOLOG.

William Lutwiniak was always Mr. Lutwiniak to me: a benign but rather distant front-office figure to whom I submitted the typed pages of CRYPTOLOG each month and from I got them back, almost invariably, with a sweeping "O.K."

A severe budget cut had suspended publication of the so-call "underground press" of DDO—four small struggling periodicals, or aperiodicals, as they often turned out to be. Readers grumbled to me as the editor of one of those publications. So I proposed combining them into a single publication to be produced in P16. It is a tribute to Mr. Lutwiniak's persuasive powers that he succeeded in his advocacy.

The *NSA Technical Journal*, of course, had existed forever, and it was a great coup to have had something published in that professionally printed periodical, and distributed not only within NSA but also in collaborating agencies. But the *NSA Technical Journal* was not for all, being heavily biased towards mathematics in its more abstruse forms. (A typical title, which lives in my memory, is "A Random Walk along a One-dimensional Lattice.")

The mass of practitioners in our various fields needed a less imposing and more responsive forum, in which they could share their knowledge and plead their causes, and this forum CRYPTOLOG provided. It also allowed for some family-style discussions on agency policies, and an occasional bit of humor, all with Mr. Lutwiniak's cheerful support.

I have long since been banned from reading CRYPTOLOG, but I'm glad to learn from collateral sources that it still flourishes, bigger and better than ever, a lively part of William Lutwiniak's legacy. ~~FOUO~~

CLASSIFYING YOUR PERSUM

Richard D. Sylvester, B Group CAO

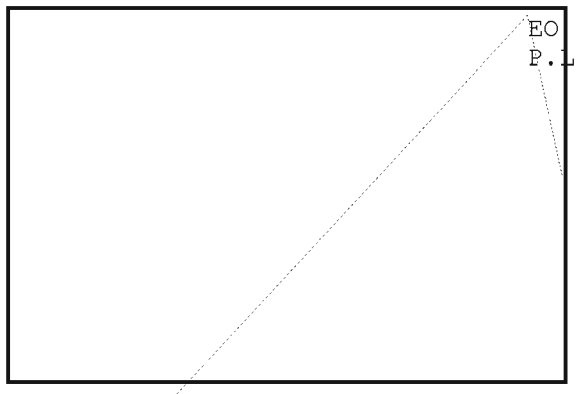
(U) Civilian Personnel Summaries (Form P3267) are strictly formatted, and for this reason it is often cumbersome to employ portion marking procedures for all the information contained therein. Nevertheless, if standard portion marking cannot be applied throughout, you should devise a method to clearly indicate the classification level of all information inscribed. Normally, the information entered in blocks 8 (Summary of Current Assignment) and 9 (Summary of all Previous Civilian and Military Service of a Cryptologic Nature) is in narrative form and it is a simple matter to apply portion markings to these narrative presentations.

(U) But there may be instances wherein certain information entered in other sections of the PERSUM also is classified. They, too, should be afforded portion marking protection. For example, you may list classified publications you have authored in block 12. If the titles of the publications are classified, you should, in parentheses, cite the classifications following the titles. In the case of certain field assignments in block 10 that require classified handling (discussed below), this information also should be marked in the most coherent and discernible manner possible.

~~(TS-CCO)~~ For example, in the first column of block 10, you might list the organization to which you were assigned

~~(TS-CCO)~~ There are certain other factors to be considered when composing your PERSUM: You may include information classified up to and including Category III COMINT (TOP SECRET UMBRA). But PERSUMS should not contain information that requires compartmented handling such as TK, BYEMAN, GAMMA, LOMA, etc. The reason for this restriction is obvious: the individuals who may be required to review your PERSUM may not be cleared for these special accesses.

~~(TS-CCO)~~ Certain field sites to which NSA personnel are assigned may also classified. If you specify in block 10 of your PERSUM that you, as an NSA employee, have been assigned to one of the following field sites, you must assure that your PERSUM is classified, at a minimum, in accordance with the classification specified.
To cite just a few examples:

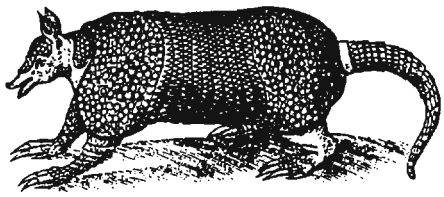


(U) Finally, you must affix an overall classification at the top and bottom of each page of your PERSUM, on the lines indicated for classification, commensurate with the highest classification of information contained within the PERSUM.

(U) Be sure your PERSUM is appropriately classified!

(U) In addition to neatness, brevity and accuracy, certain reviewing officials may judge you on the proper classification you have assigned to the information set forth in your Personnel Summary. Consult your element Classification Advisory Officer for assistance in classifying this most important document.

Shell Game



P.L. 86-36 [redacted] *P0433*

I hope to make this column a regular feature of CRYPTOLOG once again. It has been absent since the retirement of the original author.

It started as a tipsheet on using UNIX shells in the early days of PINSETTER development. At that time UNIX was relatively new to the Agency, so any tips were well received. Now we've advanced well beyond that stage, so I would like to use the column as an information exchange.

For those who may not know, PINSETTER is a P14 project to develop software tools for traffic analysts. It has come to be closely associated with the UNIX environment simply because that is the development platform we eventually settled upon. We use the UNIX shell extensively to package the tools into processing cycles. As most of the tools are simply data handlers and manipulators, they are often useful to disciplines other than traffic analysis. So we are using the pages of CRYPTOLOG as a way to reach the entire analytic community .

[redacted]

We've recently implemented a software distribution scheme for PINSETTER that takes advantage of [redacted] capabilities. Call [redacted] on 963-3369s for instructions. Network

[redacted]

A revised basic PINSETTER manual pages will be available shortly. At present several PINSETTER and UNIX-related tutorials are available. Among the titles: *How to Use SED* (October 1988), *How to Sort* (April 1991), *How to Search* (August 1991), and *How to Rearrange* (November 1991). Contact P0433 on 963-3369s for copies.

Letter

To the Editor:

I have just read *Improving NSA's Processes: Looking at the Problems*, published in January 1992. This document conveys a great deal of interesting information about the Agency. So does the photograph of senior Agency personnel on the cover: nineteen men and one woman. Moreover, that lone woman is doing double duty as a female and as a minority.

The picture is even worse when you look at the composition of the task force for the various subjects: planning, financial, and so on. Even the task force for the SIGINT production process has only one woman among the seven members.

Vera Filby, D9

SIGINT in the Novels of John le Carré

[redacted] *G41* P.L. 86-36

(U) The nine espionage novels John le Carré has written since 1964 have been widely read and analyzed on many levels—authenticity, political slant, and even literary symbolism. This article will look at the ways in which SIGINT has been portrayed in those novels—how often, how accurately, and to what effect. It will also demonstrate that while le Carré has often found it handy to use SIGINT as a plot device, he does not hold SIGINT or the other technical intelligence disciplines in particularly high regard. Rather, he is a fervent partisan of HUMINT and a persistent critic of the technical disciplines and the people who practice them. A warning: the article will summarize some of the plots of these superb stories, so stop here if you intend to read them in the near future. (One ending is revealed here only because of the role played by SIGINT in the novel's outcome.)

(U) There are no SIGINT references at all in le Carré's breakthrough 1964 novel *The Spy Who Came in From the Cold* nor in his third novel, *A Small Town in Germany* (1968). But SIGINT does play a key role in his second novel, *The Looking Glass War* (1965), which was much less successful both commercially and critically. In this book a decrepit intelligence department of the British Ministry of Defence undertakes to train an agent and infiltrate him into East Germany to check out tenuous reports of Soviet missile deployments there. The department hasn't run agents since WW II, but hopes that a success will put them back in business and increase their budget and influence. Out of touch with contemporary tradecraft and operating on a shoestring, they engage a WW II agent who became a garage owner after the war. One of the planners asks George Smiley if MI6 will loan them modern short duration signal agent comms gear for a "training exercise." When Smiley says that he cannot risk compromising new equipment and techniques, the MOD man says they'll have to use a WW II-era agent radio and asks Smiley how often a transmitting agent must change frequencies in order to foil direction-finding. Smiley says "every two or three minutes," but warns that there are several other factors—"luck, reception, amount of signal traffic, and density of population."

(U) After refresher courses in marksmanship, unarmed combat, German, missile technology, ciphers, and communications, the agent "Mayfly" crosses the border carrying an ancient and heavy HF radio in his suitcase. His first transmission is so slow and clumsy that the listening Vopos initially believe it's a child rather than an illegal agent. A U.S. SIGINT site in West Germany also intercepts Mayfly's report, and the Americans ask MI6 if it's one of their agents. The head of MI6 sends Smiley to the safehouse on the German border; Mayfly has killed a sentry, which has given the MOD cold feet, and, now, caught in an unauthorized operation, they agree to close it down. When Mayfly makes his next transmission, only the East Germans and the Soviets are listening. He's easily located by D/F and captured (or killed). The British govern-

ment disowns him and issues a plausible denial. In the final cynical twist, Smiley learns that MI6 knew all along that the MOD was running a real operation and allowed it to continue in the hope that it would fail and keep the Ministry out of the HUMINT business forever. Le Carré has since said that this book was heavily influenced by the Bay of Pigs disaster.

(U) In 1974 le Carré published *Tinker, Tailor, Soldier, Spy*, the first of a trilogy in which Smiley pursues the Soviet mastermind Karla, head of the KGB's Thirteenth Directorate. This is also the book which showcases le Carré's many colorful eumphemisms for intelligence functions and personnel, some of which have been widely adopted by the American and British media to describe the intelligence business. In *Tinker, Tailor* he also locates British SIGINT organizationally for the first time and names its practitioners—"wranglers." It is apparently a division within MI6, comparable to the dirty-tricks people ("scalphunters"), the bug detectors ("ferrets"), the forgers ("shoemakers"), and the operations support people ("lamplighters").

(U) *Tinker, Tailor* is concerned primarily with Smiley's search for a high-level mole in MI6, recruited by the Soviet superspy Karla and run under his direction. A key element in the search is analysis of a failed operation in Czechoslovakia in which a British agent was shot and captured. When Smiley interviews the man who was duty officer during the operation, the man recalls having been informed by one of the wranglers that "all hell had broken loose on the Czech air: half of it was coded, but the other half was *en clair*. He kept getting garbled accounts of a shooting near Brno." Later Smiley reminisces about meeting Karla in 1955 in New Delhi. Karla had gone to California to activate a dormant agent network and to establish its radio communications with Moscow Centre. A coding mistake on the Moscow end allowed the British cryptanalysts to break the system. When Karla traveled to New Delhi to assess a potential Chinese agent, the Americans allowed him to leave, rolled up his agents, and had the Indians arrest him. Smiley visited him in his cell and suggested that he come to England and tell all; Moscow would blame him for the fiasco in the U.S. and he faced a bleak future at home. But Karla spurned the British offer. The Indians then deported him to Moscow, where he outmaneuvered the boss who wanted his head, had him shot, and replaced him. After that, Smiley notes, Karla never again used clandestine radio communications, and never allowed his field agents to use them either.

(U) An interesting aspect of this story is the way the mole manipulates compartmentation procedures. In 1971 the Soviets begin giving the mole relatively high-grade intelligence, and he tells three other top MI6 executives (whose assistance he'll need) that it comes from a source—"Merlin"—who will deal only with him. This accomplishes two things. First, Merlin's success puts one of the three executives, an unsuspecting and pliable man, on the fast track to head MI6. It also gives the mole a reason to meet regularly with the KGB officer who is actually running him. Smiley realizes that Merlin is the key and that the mole must be one of the four top executives privy to the compartment. The rest of the novel follows Smiley as he tries to determine which of the four is the mole. In this sense this is a cautionary tale about excessive compartmentation.

(U) The next novel, *The Honourable Schoolboy* (1977), finds Smiley, after exposing the mole and uncovering the dry rot within the service, running MI6—"appointed the captain of a wrecked ship." Some believed that they had heard "the last beat of the secret English heart." One London rumor had it that it was the Dutch SIGINT service which was really responsible for identifying the British mole, by breaking a Moscow Centre code. Believing that every activity of the service was compromised, Smiley "scraps the lot," including the SIGINT service. He describes it as having been "working practically full time for Karla for the last five years." We also learn that SIGINT operations were run from a headquarters in Bath and paid for by Foreign Office funds.

(U) Smiley's task at the beginning of 1974 is to rebuild the service and to produce intelligence that will induce the now very leery CIA "cousins" to return the Anglo-American intelligence relationship to its former status. He is also obsessed

with putting Karla out of business. He and his team—former colleagues sacked or descredited by the mole—begin by looking at an aborted investigation of a Moscow Centre money-laundering operation for paying agents, run out of Vientiane. The operation is now in Hong Kong, and an agent—the "Honourable Schoolboy" of the title—is sent there to run it down. Against the backdrop of the fall of South Vietnam, the Schoolboy goes all over Southeast Asia gathering information. Leaving Udorn, Thailand, after using the comms facility at the CIA station there, he passes the U.S. SIGINT facility and remembers having heard that 1,200 linguists work there.

(U) *Smiley's People* (1979) was the last of the Karla trilogy. It seems that Karla had a daughter, by a mistress he eventually sent to the Gulag when she became politically unreliable. The daughter is schizophrenic and confined to an asylum in Switzerland; Karla has been illegally using operational funds funnelled through his man in Paris for a ghost agent to pay the considerable expense involved. The man in Paris is told to use couriers whenever possible, since Karla "is against excessive use of radio." Smiley notes that Karla's earlier vow not to use clandestine radio was apparently "subject to review." An Estonian emigre living in London, a former agent of Smiley's, learns all this through a complicated chain of events, but is killed on Karla's orders before he can tell Smiley; Smiley is again brought out of retirement to investigate the murder.

A DEPARTURE TO THE MIDDLE EAST

(U) *The Little Drummer Girl* (1983) was a departure from the earlier books in terms of both location and characters. Le Carré told an interviewer in 1983 that his original concept was for a novel about the Middle East set in London and Washington, but he couldn't find a credible way to involve MI6 and Smiley and ended up making the Israelis the central characters and setting it in part in the Middle East. This novel deals with the efforts of a team of Israelis to capture or kill a Palestinian terrorist ("Khalil") whose speciality is bomb attacks against Israelis in Europe. They grab and eventually kill Khalil's younger brother Michel and recruit a British actress named Charlie to pose as a sympathizer and Michel's lover. While SIGINT plays no role in this novel, the Israeli communications gear is described in some detail. Most of the operation is supported by a mobile comms van equipped with both secure voice and enciphered printer. When forced to use clear voice, they use the callsigns and jargon of taxi companies and other legitimate users of mobile comms.

SIGINT TRAPS A "PERFECT SPY"

(U) SIGINT does play a significant role in *A Perfect Spy* (1986), which le Carré has described as his first work not submitted to Her Majesty's Government for prepublication review. It is the story of one Magnus Pym, MI6 station chief in Vienna in 1983. As the novel begins, Pym, haunted by the death of his con-man father, has disappeared. His wife and colleagues are baffled and fear that he's defected. He has in fact gone to ground in a rooming house in a coastal town in the UK, where he is writing the story of his life for his teenage son. The novel's chapters alternate between the story of Pym's life up to his disappearance and MI6's efforts to discover where he's gone and why, and to keep the CIA from learning that there may have been another major British security disaster.

(U) Pym was induced into the intelligence business after WW II by the MI6 Station Chief in Bern; Pym was studying at a university there and met the man, Jack Brotherhood, at the local Anglican church. Brotherhood uses Pym for various low-level tasks, such as collecting the names of leftists at the university and translating stolen documents. Pym tells Brotherhood about Axel, an illegal German refugee whom he has befriended at his rooming house, and Brotherhood informs the Swiss counterintelligence service in order to accumulate "barter material." They arrest Axel and deport him.

(U) After graduating from Oxford in modern languages and taking a commission in Army intelligence, Pym encounters Axel again in Austria. Axel is described to Pym as a Czech Army officer who wishes to defect, but it's a ruse. Axel proposes that he become Pym's agent and gives

him a great deal of classified information to establish his bona fides. Soon Axel tells Pym that their relationship has become known and that Axel can protect himself only by making it look as if Pym is Axel's agent. To pull this off he will need legitimate classified information from Pym. Pym never seriously considers not doing it; he has vowed not to betray Axel a second time, and there is also the problem that his own reputation rests on what Axel is feeding him. (We learn later that the material Axel is providing looks good but is of little actual value.)

(U) Upon demobilization in 1953 Pym enters MI6 and is sent abroad again—to Czechoslovakia, of course. He is soon caught and pitched by Axel again. This time, Axel says, they'll make each other into intelligence superstars, by "making straight for the biggest diamonds, the biggest banks." But what Pym will get from Axel over the years will be largely disinformation, supplied by nets of agents fully controlled (knowingly or otherwise) by the Czechs and other Eastern European counterintelligence services. Piling success upon success, Pym goes to Stockholm, back to London, to Berlin, and then to Washington as Deputy Chief of Station, followed everywhere by Axel. But the Americans begin to become suspicious; the Eastern European networks produce good material only when Pym (and Axel) are actually there. Pym is summoned to London for an investigation, but MI6 does only a cursory check and sends him back to Washington with a clean bill of health.

(U) The CIA keeps pushing, however, and sends a team to London to present new evidence of Pym's treason. This is after Pym has disappeared, but the British have concealed his absence from their American colleagues. Artelli, the SIGINT analyst in the American team, is described as "a distraught mathematician" from "Signals Intelligence." The new evidence is traffic analysis of clandestine communications from the Czech Embassy in Washington and from other Czech facilities in the U.S., particularly the consulate in San Francisco in 1981 and 1982. The significant point is that the transmissions stopped every time Pym left Washington, and the assumption is that they're meant for Pym and aren't broadcast when he's away. Artelli adds that the communications techniques are old-fashioned and give off a "sense of long habituation, one human being to another." Although the communications are unreadable, the cryptanalysts know that the keys are derived from some kind of text. Artelli also reveals that there are strange things going on with Czech clandestine radio in the last few days—the equivalent of blind calls to someone.

(U) The Czechs, like the British, are trying to find Pym, although the CIA doesn't make the connection because they don't know that Pym is missing. Then another team member brings up more new evidence—the travels of a Czech intelligence officer named Hans Albrecht Petz, AKA Alexander Hampel, AKA Jerzy Zaworski. Petz is Axel, of course, and his travels in Europe and the U.S. coincide perfectly with Pym's. The British still refuse to believe it, arguing that the Czechs have mounted an elaborate deception to discredit someone who's been particularly effective against them. Their ambiguity about where Pym is and what he's doing convinces the Americans that he's flown the coop. Brotherhood, still in MI6, finally comes to believe Pym's treachery, and learns from Pym's wife that Pym takes a battered copy of a 17th-century German book entitled Simplicissimus everywhere he goes. The book (actually Der Abenteuerliche Simplicissimus Teutschroughly, (*The Adventures of a Simple German*) was given to Pym by Axel when they first met in Bern, and it's a somewhat heavy symbol. The author, Johann Jakob Christoffel Grimmelshausen, fought on both sides during the Thirty Years War, and used many pseudonyms which were anagrams of his name. Brotherhood tells the British SIGINT service to run the Czech clandestine traffic against the book, and it works.

(U) Now everyone is looking for Pym—his wife, the British, the CIA, and Axel, who fears he is suicidal and wants him to defect to Czechoslovakia. The CIA Station Chief in Vienna, an old friend of Pym's from Washington now obsessed with nailing him, has enlisted his own wife to help watch Pym's wife there, and she sees Axel contacting his wife in a church. She immediately calls her husband at the U.S. Embassy in London on an open phone and tells him with a clumsy prearranged code. The British,

who have tapped the embassy phones, intercept the call. But Pym's wife evades both the Americans and the British, makes it back to England, and tells Brotherhood that Axel has unknowingly let her know where Pym probably is. The book reaches its climax as all the interested parties rush to reach Pym first.

A COMMUNICATIONS DECEPTION

(U) SIGINT plays a small but important role in le Carré's 1989 novel *The Russia House*. It is his Glasnost novel and his most political book to date. The central character is one Bartholomew "Barley" Blair, an alcoholic British publisher and saxophone player. A dissident Soviet scientist who met Barley briefly at a party tries to have a manuscript delivered to him via a Moscow book fair; it eventually ends up at MI6. According to the manuscript, Soviet military technologies—particularly missiles—simply don't work. The Soviet military research establishment has not only produced weapons that don't work, they've faked the test results to conceal the failures from their own government. The scientist, one Yakov Savelyev, wants the manuscript published in the West, believing it will lead to large-scale disarmament on both sides. The British and the Americans have another idea, of course. Their biographic research reveals that Savelyev—now code-named "Bluebird"—is responsible for, among other things, telemetry encryption. Part of what he has provided is the original telemetry—before it was faked and before it was encrypted. They want to use Barley to determine whether the material is genuine and then have Barley run Bluebird as an agent in place. Against all his instincts, Barley agrees to do so.

(U) After three weeks of training Barley goes back to meet Savelyev in Leningrad, takes more material from him, and promises him he will get the manuscript published. Barley then travels to the U.S. for a combination debriefing and interrogation by the CIA, now the senior partner in the operation. A senior CIA official warns Barley and the British that the American military-industrial complex doesn't welcome the Bluebird manuscript and will work hard to discredit it.

(U) Barley returns to Moscow with a shopping list of questions for Savelyev, and the CIA smuggles in a truck full of "surveillance" gear to monitor developments. The British officer who has been functioning as Barley's case officer (identified only as "Ned") begins to get cold feet, aware that the Anglo-American shopping list tells the Soviets everything we don't know about their strategic weapons programs—and, by inference, everything we do know. The rest of the team ignores his concerns, convinced that everything is on track. But Ned is right—Savelyev has been caught and turned. Meanwhile, the Soviets practice a bit of deception to ensure that they'll get the shopping list. A Soviet military entity in Leningrad sends a message to Moscow authorizing Savelyev to take a recreational weekend there after he delivers a lecture; it is intercepted by a U.S. SIGINT facility "in Finland" and decrypted. The Americans and the British buy it, although Ned suspects it was planted. He points out that it was enciphered by an ancient Soviet machine and that there are no other messages intercepted like it. Barley delivers the shopping list and then disappears, a good juncture at which to end this plot summary.

GEORGE SMILEY'S VALEDICTORY

(U) *The Secret Pilgrim* (1991) features the first appearance of George Smiley since *Smiley's People*. Ned of Russia House was made the scapegoat for the Bluebird fiasco and exiled to run the MI6 agent training school. He invites Smiley, his mentor and father figure, to talk at the graduation dinner of a class of agents, and Smiley agrees to do it. Every anecdote Smiley tells reminds Ned of an operation of his own, and the book is basically a collection of Ned's vignettes from three decades of espionage. There are no references to SIGINT as such, but in the stories both the British and the Soviets continue to rely heavily on clandestine radio through the 1980s.

(U) What can we say about le Carré's apparent knowledge of SIGINT from this review of the novels? To use the Watergate question, what did he know and when did he know it? He seems to have a good grasp of clandestine radio techniques and counter-clandestine SIGINT capabilities. If there is a tradecraft moral, it is that "agents

shouldn't use radio." "Mayfly" in Looking Glass War, Karla, and Pym are tripped up by successful counter-clandestine SIGINT operations. Le Carré does not display much awareness of broader SIGINT applications, such as on political, economic, and military topics. This is consistent with what is known about his intelligence career—he was a case officer in the 1950's and 1960's and would probably not have had regular access to mainstream SIGINT reporting. There is also the matter of censorship by the British government; le Carré claims that he submitted every novel prior to *Perfect Spy* for pre-publication review. It is unlikely that official reviewers would have allowed any accurate information about British or American SIGINT activities to be published. In this regard it is interesting to note that no le Carré novel has ever referred to "NSA" or "GCHQ"; this could not possibly have been because he didn't know about those organizations.

(U) People involved in any of the intelligence disciplines have an ambivalent attitude towards having their craft described in fiction. On the one hand, we sneer at the more lurid and fanciful fictional descriptions of our profession; on the other hand, we are appalled and often want legal action taken against writers who get it right. So in this sense, as SIGINT professionals we should be happy that le Carré's references to our business are few and mostly uninformative.

HUMINT vs TECHNICAL INTELLIGENCE

(U) But le Carré has another agenda which is more interesting. He is not only a strong partisan of HUMINT as an intelligence discipline, but he actively disparages the other more technical means of collection and analysis. He is to intelligence as the 19th Century Luddites were to the industrial revolution—a rabid foe of technology. This is manifested in several ways in the novels which may not be readily apparent from these brief plot summaries. For one thing, he portrays intelligence technologies as peculiarly—and offensively—American. Some of the most despicable characters in his books are British officials who make deals with the CIA to share the fruits of American intelligence money and technology. His heroes are HUMINT practitioners who detest depending on Americans and scorn nearly all uses of technology. Alleline, the mole's pawn in *Tinker, Tailor* adored Americans, while MI6's Director, Smiley's beloved father figure, detested them and all their works. The mastermind in *Little Drummer Girl* was described as out of tune with Mossad's polygraphs "and their ever-growing faith in American-style power plays, applied psychology, and crisis management." The noble Jack Brotherhood in *Perfect Spy* objected to MI6's pandering to American "methods and example." Conversely, the people in his novels who are good at technology are often unpleasant characters. One particularly nasty MI6 officer in Russia House was described in this way: "Clive was a technology man, not at ease with live sources, a suburban espiocrat of the modern school. If he liked anything at all in life apart from his own advancement and his silver Mercedes, then it was hardware and powerful Americans, in that order." For Clive, human nature was "one vast unsavory nightmare." In *Secret Pilgrim* Ned, in praising the successes of an MI6 officer against the Khmer Rouge, notes that espionage technology "can't break the codes of an army without radios." Ned also reflects with nostalgia on a time before MI6's registry was computerized, when it "could still find what it was looking for, or know for sure that it was lost."

(U) Le Carré has developed this theme even more explicitly outside of his fiction. In a 1986 interview he attributed what he called the "flagrant failures" of Western intelligence to an "obsession with high-tech espionage." In a 1989 interview he said that "the shift of professional confidence from human assets to electronic ones is a direct consequence of U.S. domination of Western intelligence." He went on to say that when human agents are well recruited and well targeted, "they are affordable and often far more reliable than the inductive fantasies which result from the reading of signals and codes and photographs."

(U) There are several possible explanations for le Carré's animus against the technical intelligence disciplines and their practicioners. One is that it's a manifestation of an obvious anti-American bias, although he adamantly denies that he's anti-

American and cites as evidence the number of obnoxious and incompetent Brits who appear in his novels. This means, he says, that he's even-handed. Although the reader will have to make his or her own judgment, it seems to this writer that criticism of American power and policies is a consistent theme in both his fiction and his public statements. It makes for a fairly simple equation—le Carré scorns SIGINT and imagery because they are dominated by the U.S.; they exemplify American technological arrogance.

(U) Another explanation may be that he has never really been exposed to SIGINT and imagery and doesn't understand their value or their complexity. A senior CIA HUMINT officer who came to NSA in another capacity as a retired annuitant told this writer that for his entire CIA career he thought that all NSA employees were like the State Department communicators he encountered in embassies—skilled communications technicians. This person was astounded to learn what we actually do in terms of signals processing, cryptanalysis, language work, and analysis. There are also people who disdain technology because they don't understand it and secretly fear it; it wouldn't be surprising if an early 1950's graduate of Oxford in modern languages harbored such attitudes. The answer may well be a mix of all three.

THE MORAL COST OF HUMINT

(U) What is striking about le Carré's relentless public championing of HUMINT is his refusal to acknowledge its human and moral costs. The relative morality of intelligence activities is a complex question. The current U.S. official position is that some acts are so odious that they cannot be justified even when they would advance the national interest; an example is the apparent prohibition on assassinating foreign officials. (The purist may argue that assassinations, like covert actions, have nothing to do with intelligence, but past involvement in assassination attempts has blurred the distinction.) Acts less grave than assassinations that would otherwise be considered immoral and/or illegal are deemed acceptable if done in the national interest. There are dissenters on both sides of the political spectrum, of course. For some on the left, such acts can never be justified by invoking the national interest. For some on the right, there are no acts which cannot be justified if the threat to the national interest is sufficiently grave. (This is similar to the theological debate about a"just war.") A middle ground might be that there should be some proportionality between the gravity of the activity and the expected benefits—one should probably not blackmail an official of a foreign government to acquire the annual projection for rutabaga production. One way to measure the relative morality of various intelligence activities might be to assess their potential for harming individual human beings. The technical intelligence disciplines have little or no impact on human beings; HUMINT, by definition, involves the exploitation of people and carries a high risk of harming them.

(U) Le Carré's failure to address the human costs of HUMINT is striking precisely because his novels are intensely concerned with questions of personal morality. As William Buckley noted in a 1983 review,"" 'The Little Drummer Girl' is about spies as *Madame Bovary* is about adultery or *Crime and Punishment* is about crime." There is endless agonizing in these novels about the moral dilemma of the case officer, whose task it is to obtain information by corrupting or seducing vulnerable human beings. Smiley speaks in *Honourable Schoolboy* about having to be "inhuman in defence of our humanity, harsh in defence of compassion, single-minded in defence of our disparity." The Schoolboy himself recalls Smiley speaking at the MI6 training school about being grateful that intelligence service provided the opportunity to repay one's country, but the Schoolboy notes that "the paying is actually done by the other poor sods."

(U) There is a strong sense in le Carré's novels of what has come to be called by conservative American commentators the concept of moral equivalence—that if those who act on behalf of the West and the USSR both commit immoral acts, there is no real moral difference between the two. As George Will put it, "In [le Carré's] espionage novels the 'ambiguity' consists primarily of the idea that means as much as ends reveal where, if anywhere, justice lies in political conflict." So a

case can be made that it's inconsistent and perhaps even hypocritical for a man so concerned with moral questions to uncritically promote the intelligence discipline most likely to harm individual human beings.

WHY THESE NOVELS MATTER

~~(C)~~ Since le Carré's writings and public pronouncements (whether because of ignorance, discretion, or censorship) don't appear to pose any threat to SIGINT sources and methods, does it matter to us what he writes? It matters because it adds to a public mystique about HUMINT that has a real (although intangible) impact on the way the Intelligence Community is perceived both by the public and by the rest of the government. Many former intelligence officials and other commentators have relentlessly pushed the idea that "American intelligence" was crippled when then-DCI Stansfield Turner cut 820 CIA Operations Directorate billets (none overseas) in the 1977 "Halloween Massacre." Although the CIA and the rest of the Community continued to perform well after this event, some have gone so far as to suggest that some major U.S. foreign policy mistakes in the late seventies and early eighties were due to this modest reduction of HUMINT assets. In a more recent example, the Congressional committees responsible for the intelligence budget added money for CIA HUMINT operations for both FY91 and FY92, while reducing the rest of the National Foreign Intelligence Program. In a perfect world decision makers should be so well informed that they couldn't possibly be influenced by an Ian Fleming, a John le Carré, or a Tom Clancy, but in this imperfect world it sometimes happens.

~~(C)~~ It is hard to develop an appropriate awareness in the right places of the actual and potential contributions of the SIGINT system without putting ourselves out of business. It was one of the primary reasons for the establishment of J8, the Office of Corporate Representation, and it would make a good subject for a separate article in this publication. In the final analysis, we're obviously better off that a writer as widely read as le Carré doesn't write accurately about SIGINT. But it is galling to know that his books and public comments make marginally more difficult the task of ensuring that resources are allocated within the Intelligence Community on the basis of real contributions instead of on the basis of myth and mystique. It is also ironic that the CIA would benefit from all this in even a small way, since le Carré has made his distaste for that organization so obvious.

REFERENCES

Monaghan, David. *The Novels of John le Carré.* New York: Basil Blackwell, 1985.

Le Carré, John. *The Looking Glass War.* New York: Coward McCann, 1965, p. 170.

—— *Tinker, Tailor, Solider, Spy.* New York: Alfred A. Knopf, 1974, p. 223.

—— *The Little Drummer Girl.* New York: Alfred A. Knopf, 1983, p. 28.

—— *A Perfect Spy.* New York: Bantam Books, 1987, p. 175.

—— *The Russia House* New York: Alfred A. Knopf, 1989, p. 89.

—— *The Secret Pilgrim.* New York: Alfred A. Knopf, 1991, p. 211; p. 179.

—— *The Honourable Schoolboy.* New York: Bantam Books, 1978, p. 461; p. 489.

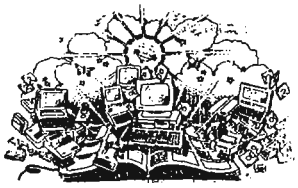
Lelyveld, Joseph. "Le Carré's Toughest Case," *New York Times Magazine*, March 16, 1986, p. 90.

Trueheart, Charles. "John le Carré, the Spy Spinner After the Thaw," The Washington Post, May 25, 1989, p. D1.

Buckley, William F. Jr., "Terror and a Woman," New York Times Book Review, March 13, 1983, p. 23.

Will, George. "Le Carré's Unreal Mideast," The Washington Post, April 28, 1983, p. A13.

Technical Literature Report



Communications, Computers, and Networks:
The September 1991 Special Issue of
Scientific American

P.L. 86-36

Reported by: [redacted] *W31*

(U) Once a year, Scientific American publishes a single-topic special issue. The 1991 special topic is Communications, Computers, and Networks. It is "required reading" for analysts in a number of fields, not just computer science.

~~(S-CCO)~~ The structure and use of high-capacity computer networks is covered in various articles. This includes network protocols, packet switching, and projections for the future of networks. The consensus is that the use and capacity of networks will grow tremendously in the next decade. Senator Al Gore writes that networks will be as important to the competitiveness of America as the interstate system was during the 1960's and 1970's. (He has gone so far as to introduce the High-Performance Computing Act of 1991, an attempt to create a national high-speed fiber optic network.) [redacted]

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

(U) The discussion of networks is entwined with that of communications. Various types of data communication are currently carried via computer networks—everything from E-Mail to graphics. Several writers see that the distinction between the telephone, television, mail service and other means of messaging is becoming increasingly blurred.

~~(S-CCO)~~ One of the most intriguing possibilities is that of virtual reality (VR). By the use of electro-mechanical feedback, special viewing goggles, computers, and high-speed networks, people can not only watch "the action", but they can become part of it as well. [redacted]

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

~~(S-CCO)~~ Another interesting topic is ubiquitous computing currently in use at the Xerox Palo Alto Research Center (PARC). There, the network pervades the workplace. Via the use of infra-red and radio relay, people can carry small computer "notebooks" which are in constant communications with mainframes, workstations, other notebooks, printers, and even "smart" active badges. The display on the notebook is customized automatically to fit the needs of whoever is currently using it; this is done via the active badge. At NSA, an employee's badge carries a picture and PIN for the wearer. At PARC, the badge carries data files, wearer identification and location, voice communications, and can even forward phone calls to the right room. The use of such a system at NSA could be a mixed blessing. (People would never be out of touch with their office. But then, it would be harder to dodge unwanted phone calls!) [redacted]

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

(U) There are othere topics of interest to us in the special issue, such as data security, cryptography, and the legal ramifications of the use (and abuse) of large scale national and global networks. Reading this issue can help understand some of the possible intelligence challenges of the 21st century.

International Technical Communications Conference, 13-17 April 1991, New York

P.L. 86-36

Reported by [redacted] *A64, et al.*

Many NSAers spend some time writing and editing documents of one kind or another. While our audiences and topics may vary from office to office, our responsibility does not. The information that we are tasked to communicate is of vital importance. Therefore we have an obligation to produce documents of the highest quality possible—models of accuracy, clarity, succinctness, and elegance, easily grasped and gentle on the eyes. This standard is a difficult and elusive one, achieved only through great effort and no little study.

With this in mind, a contingent of writers and editors from NSA attended the 38th Annual International Technical Communications Conference in New York City, sponsored by the Society for Technical Communication. The conference attracts technical writers, editors, designers, and managers from all over the world. The three days of sessions featured over 185 seminars on various aspects of writing and editing, research and technology, visual communications, and management.

I. BENEFITS OF ATTENDING SUCH A CONFERENCE

It has been said that NSA's SIGINT reporters are at a disadvantage because unlike mathematicians and linguists, there is no outside professional society for them. This is not quite true. Actually, there are several for journalists, though membership in them is inadvisable. But there are two professional societies of writers, editors, and audiovisual presenters that can provide guidance on presenting information: the STC, whose conference is reported here, and the National Association of Government Communicators.

NSA is at a disadvantage in selling our product for two reasons: one, is that CIA has several years' start on professional-looking publications, thanks to the mandate of a senior official who demanded and got professionals experienced in publications to set standards. Since then, the homespun look of our product has tended to diminish its authority, though we may believe that our product has more validity. Another is that the new DCI is emphasizing HUMINT and de-emphasizing technical intelligence, DESERT STORM notwithstanding. So we must take still another hard, critical look at our publications. We must not fall behind in the very competitive intelligence arena. Presentation is all.

A very large conference like this is ideal for getting a quick update on what everyone else is doing. First of all, there is a lot to learn about the new editing, writing and layout techniques that are based on scientific experiments: electrodes are implanted in the brain to track eye movements and test message understanding. From these experiments new rules have evolved.

Then, from discussions at the sessions and from chatting during coffee breaks you may begin to develop an appreciation for the norm: what is usual, what editors and writers are expected to do in other organizations, the degree of freedom in substantive matters, in management, and in personal relationships.

The specific topics of interest to our group were those dealing with the nuts and bolts of document production: the basics of communication, editorial responsibility, managing the editor-author relationship, how to tailor documents to meet the needs of intended users, page layout and design, and document maintenance. In the course of these three very intense days of lectures, workshops, exhibits, and panel discussions, we gathered a great deal of information. Following is a summary of the information presented at the sessions attended.

II. COMMUNICATION AND EDITORIAL RESPONSIBILITY

Effective communication consists of five basic steps:

1. research—ascertaining exactly what the customer needs and wants, and identifying potential users;

2. planning—how to achieve objectives;

3. collection of pertinent, useful information;

4. composition of concise, consistent, and understandable prose from often diverse sources; and

5. final presentation of accurate material in a user-friendly format.

In the course of this process, a communicator often acts as coordinator, synthesizer of information, editor, designer, and, very often, producer of ideas for new documentation. With its many demands, modern communication is a challenging task with a number of potential pitfalls. For example:

• ***Implementation at the expense of planning.*** The pressure to produce to meet a deadline often precludes this essential preliminary step. Important factors may be minimized or completely overlooked. Effort taken to identify and plan for potential problems early on can save valuable time in the latter stages of production. You must communicate with customers to find out exactly what they want. Avoid ambiguous tasking; make sure that job requirements are explicit. Also, ***get them in writing***.

• ***Depersonalization.*** Ease of collection and manipulation of data can lead to neglect of the needs, values, perspectives, and biases of both the people who supply the information and those who will ultimately use it. Know the people behind the work—in other words, ***be sensitive***.

• ***The Hothouse Effect.*** This results from a lack of feedback or input from people from other organizations, publications, etc. The consequence of this insular approach is complacency and a tendency toward self-service, which ultimately renders your work useless to anyone else. Canvass others for input, opinions, ideas, and feedback. Find out what is important to them. Exchange ideas, concerns, and technologies with people with similar interests and experience. Generally speaking, when you go into any interaction with people, be prepared to learn something from them. Chances are, you won't be disappointed.

• ***Technological guilt.*** This is defined as sacrificing the needs of your users to a self-indulgent fascination with the many "techno-toys" on your desktop publisher. It can lead to an abuse of available capacity, user disservice, and compromised communication. Don't use all the fancy gimmicks available to you just because they are there. Decide what best meets the requirements of the document and its potential users, and design accordingly.

• ***Premature buy-off.*** This is the tendency to underdevelop material for the sake of getting the job done. Don't allow others' expectations or uninformed perceptions of required time and effort force you into an unrealistic production schedule. Objectively assess what it will take to use the material to its best and fullest advantage, then proceed from there. *Also, don't bite off more than you can chew.* If you can't do the job with the time and resources allocated to you, say so!

Remember that the primary goal of communication is to convey information in the clearest, most precise and succinct manner possible.

Take Positive Steps

To further this goal, a communicator should keep in mind these important points:

• ***Make communications as usable as possible.*** Anything that helps users acquire information easily is a worthy tool for the technical writer: extra leading and/or kerning, more graphics, larger type, a bigger trim size, wider margins, spiral binding instead of perfect, etc.

• ***Take an active role.*** Don't let your customers push you around. If you don't think the job can be done, *tell them.*

• ***Talk to people.*** Talk to your sources, users, colleagues in the field. Find out what they know, what they think is important, what they like, what they don't like, etc.

• ***Be curious.*** Try to take an interest in what you're writing about. If you're not interested, your writing will suffer.

• ***Avoid complacency.*** Ask, listen, be informed; be open to new ideas and procedures.

• ***Resist specialization.*** Cultivate a diversity of experience. Produce materials on a variety of subjects, in a variety of styles (within reason, of course). Accept new challenges. Above all, be a team player. Accept success (and failure) as part of a team effort.

• ***Be humble.*** Remember: You can *always* learn—from anyone!

Working with Authors

In addition to their aforementioned responsibilities, communicators are often called upon to act as editors whenever it is necessary to incorporate the work of others into their documents. In this context, a whole new set of skills is required, perhaps the most important of which is the ability to work effectively with authors.

The purpose of the editorial process is to help authors communicate their ideas in the clearest, most concise manner possible, while at all times preserving the character and integrity of their individual styles. Whatever contributes to this process lies within the scope of the editor's task. There are a few points to remember regarding this principle:

• ***Learn to submerge yourself.*** Don't allow personal biases to skew your treatment of others' work. Try to operate consciously at many different levels. For example, try to imagine yourself as the author, expressing ideas that mean a lot to you. Imagine yourself as the reader, trying to make sense of difficult concepts. Develop a sense of perspective, that is, other people's.

• ***Know that editorial skills are tools.*** And, like tools, they are to be used to perform a specific task—in this case, to help authors communicate most effectively. Any other use constitutes abuse. Also remember—

Editing is only a part of the system, comprising all the other elements of document production: proofreading, design, typesetting, art work, printing, binding, etc.

It is easy to make mistakes. That is why the world (whether or not it wants to admit it) needs editors. The point? Be nice, be patient, be sensitive, be diplomatic. Being the "victim" of an edit is often a painful experience. People do not like having their mistakes pointed out to them or their masterpieces carved up. Also, editors, being human themselves, are liable to make mistakes. Try not to err, but, if you do (and you will eventually), learn what you can from the experience, then *forget it.* Learn to forgive yourself, as you forgive others.

Things are not as simple as they appear. Respect what you edit, whatever it is. Carefully examine the job to determine how best to treat it. Let other editors read the original for their assessment before you edit, then give them your edited version for comments and suggestions.

Some Common Editing Styles

• ***Editing by whining.*** This is defined as letting authors get away with murder (in this context, illiteracy) and then complaining that their work is bad. Don't let authors push you around. When they're wrong, tell them!

• ***Editing by fiat.*** A few representative pronouncements associated with this one are, "I'm the editor, and what I say goes!", "Rules are rules. If you don't like 'em, lump 'em!", "What do you know? You're just the author!", etc. Sometimes known as the "brickbat method," this approach, as you might have guessed, is detrimental to the author-editor relationship. Don't do it. Respect your authors; respect their work, opinions, and desires.

• ***Editing by restraint.*** This method, a combination of the above, requires good judgement—a sense of when to say "no" and when to let things go. If something an author wants to put into a document, while perhaps technically incorrect, is sufficiently insignificant to overlook, let it go. It doesn't matter. On the other hand, stick to your guns when you know that an editorial change is an important and necessary one.

• ***Editing by instruction.*** When confronted by situations in which authors wrongly object to editorial changes, attempt to enlighten them, in a tactful, non-patronizing manner, as to why changes were made. If they remain adamant despite your explanation, do it the way they want it. Remember, it's *their* names that will be associated with the work, *not* yours.

III. PRODUCTION AND MAINTENANCE of EFFECTIVE DOCUMENTATION

"Contextual Inquiry" is a field research technique for observing users in their work environment. Before producing documentation on job-specific procedures, the writers must understand the context in which they will be applied. This will assure that documents are tailored for the intended audience. For example:

• ***Work language***—the language they use to describe what they do. Are the words you're using the same as those used by the people for whom the document is intended? If not, change your language or provide a glossary. Also,

ascertain the level of knowledge of your audience; this should determine the words you use.

• ***Work structure***—the way they do their work. How does your prospective audience work? At home *and* at the office? Just at the office? In the field? Do they work with their hands? Is their job one that can be done 8 hours a day or only for a few hours at a stretch? Do they have the time to read the documentation? The answers to these questions will determine what sort of document you produce. For example, if it's a do-it-yourself manual, you'll need a publications design that is easily accessed by someone whose hands are occupied. A flat-lying, spiral-bound document with large print and plenty of white space and graphics would probably work best.

• ***Work goals and intentions***—their overall work goals and concerns. What are the deadlines and/or constraints under which users must work? What is the ultimate goal of their work? For example, if their job requires a thorough knowledge of a given subject, a textbook-like approach might be more appropriate. Should a basic working knowledge be all that's needed, a quick reference guide with section markers would probably suffice.

• ***Work product***—the product they need to create or the task they need to accomplish. How do existing working aids contribute to the performance of their task? What is it about those working aids they like? dislike? What would they like to see in future documentation?

When you create documentation that matches users' work language, structure, intentions, and product, that documentation is said to be "usable." By using Contextual Inquiry early in the documentation process, you are more likely to produce material that is usable and meets user needs.

Steps for Conducting Contextual Inquiry

1. ***Focus.*** Decide what it is you're trying to find out. Make sure your focus is narrow enough to allow you to zero in on pertinent and useful information in your interviews with prospective users.

2. ***Select participants.*** Find representative interviewees or, if you have time, take a cross-section of the work force.

3. ***Schedule the interview(s).*** Find a time most convenient for interviewees, when they can give you their undivided attention. Schedule the interview for 2 to 3 hours each. (Any longer will tend to fatigue both parties.) Get permission to record. Make sure you can see your interviewees in their work environment.

4. ***Conduct the interview.***

• Begin with a traditional interview.

• Observe the interviewee's work and discuss ideas concerning it:
- Ask open-ended questions.
- Let the interviewee lead the conversation.
- Listen!

• Conclude the interview
- Summarize your analysis.
- Ask "pet" questions, that is, questions you think you know the answers to.

• Thank the interviewee.

5. ***Extract the Data.*** Sift through the interview for usable information, but don't alter the data in any way and don't attempt to interpret. Use the interviewee's words. Extract important points for analysis and record them on Post-Its. Stick them up where you can see them.

6. ***Organize.*** Data are organized by their characteristics and relationships. Take the bits of data (on the Post-Its) and arrange them into groups of items that seem to go together. Allow the various categories to emerge. Come up with representative names for these groups. See if any categories fit under higher-level categories.

This mass of information should allow you to draw some valuable conclusions as to how you might best serve users of your product. By learning their specific needs, concerns, work environment, goals, etc., you will write and design materials tailored-made for them.

IV. DESIGN AND FORMAT

Having developed a thorough knowledge of your audience and collected the information required of your subject, you must create a strategy for presenting the material in the most effective manner possible.

Effective documentation requires the clear and concise translation of technology into accessible communication. Information design, while not

contributing quantitatively to a reader's knowledge, can facilitate the conveyance of information by presenting it in a "user friendly" fashion.

Information design should combine attractiveness with optimum functionality and effectiveness. The design process is a three-stage one:

1. ***Planning.*** Learn your subject. Find out everything you can about it. Again, *know your audience (potential users)* and find out what *they* need.

2. ***Development.*** Come up with an appropriate design. Write the documentation. Put together a prototype. Test the document on potential users. Collate and evaluate the results, and incorporate them into the final version.

3. ***Implementation.*** Produce and publish the manual. Solicit and monitor user responses. Create a schedule of maintenance for updates and design improvements.

Issues in Developing a Design

- Is the design you're creating appropriate to the subject? What is the purpose of your documents: are they going to be a quick, easy reference guide or a detailed instruction manual?
- Is the design durable? Is it one that will work in any context at any time, or is it perishable?
- Does it have impact? Does it make the user want to read the text it's attached to?
- Is it verifiable? Can it be demonstrated, through user testing, to be most effective?
- Is it cost-effective?
- Is it accessible, that is, easy on the eyes, well-organized, and interesting?
- Does it have lots of white space?
- Is it something you *don't* notice? A good design doesn't distract the user.

Visual communication (design) can have significant impact on how effective your text is in communicating your subject to a reader. "Visual literacy" is defined as the ability to create and use design to convey information.

Some Tools for Effective Information Design

- *Chunking.* This is defined as the breaking up of information into manageable sections. Related topics are placed together in an attractive, usable manner. This can be achieved with section dividers (tabs), separate volumes, headers.
- *Queuing.* This involves creating a logical progression of information so that each chunk of data builds on that which came before it. This should be done visually; possibly the simplest way to achieve this is with different levels of headers.
- *Filtering.* A way of organizing information for quick access, this method requires the arranging of information, whenever possible, into lists.
- *Multiple access.* This is defined as mixing the above elements in a document to accommodate the myriad ways people take in information.

V. DOCUMENT MAINTENANCE

Once you have produced your manual and released it to the field, it becomes necessary to document its reception by the intended audience and to keep abreast of developments in its subject area. This will allow you to perform the next important step in the process of producing documentation—maintenance. Maintenance in this context is defined as the revision of documentation for the purposes of keeping its information current, correcting mistakes, and/or incorporating user feedback to create a better product.

There are five basic steps for revising and rewriting manuals:

1. Preparation

- If need be, acquaint yourself with the subject of the original manual. Do some research.
- Look at the original type specifications and style sheets. See what was done before. If you don't like something, change it.
- Get training and input from subject-matter experts. If you don't feel you know enough about the subject (even after researching it), find people thoroughly versed in that area and pick their brains.
- Look at how the old manual is organized. Discard this organization if you feel it's not working. New information may require a change in the way the document is structured. Also, examine the current manual's table of contents; this, too, is a good indication of how the manual is organized and what it's about. Looking at the table of contents, you can tell

whether or not the document was chunked properly.

• *Solicit and document user feedback on the old manual.* Make sure you incorporate as much of this as possible into your revision.

2. Reading Phase: Read the original manual, then ask yourself the following questions:

• Does each chapter achieve what it sets out to do?

• Is there any text that just does not seem to belong where it is?

• Are any of the concepts confusing?

• Is any of the information outdated?

• Are the chapters properly laid out?

• Can you identify the target audience?

• Is it indexed? This is *very* important. A manual should have an index; it's not nearly as useful without one.

3. Research and Verification Phase: Get answers to those nagging questions that still remain and verify what information you have already. Refer to your subject-matter experts.

• Prepare your questions for these people in advance.

• Find a quiet place and a good time when they can give you their undivided attention.

• State a time limit in advance and stick to it. If you need more time, ask for it.

4. Organization Phase: Draft a new table of contents reflecting your additions and changes. Have your subject-matter experts check it out. Only they can determine if the organization you've imposed on the work is correct and the most useful.

5. Edit and Reworking Phase:

• Use your table of contents as an outline. Based on what you see there, estimate the time it will take for initial and second-party edits.

• Use a checklist of all the elements in the manual. As you proofread or edit each element, check it off and keep a record of how you treated it in a log book. This will come in handy for future revisions.

The maintenance of manuals (updating, redesigning, reorganizing, etc.) is seldom planned for or even taken into consideration. It should be, of course. If you don't plan for maintenance, chances are you'll put it off until your manual is so outdated, it requires a hurculean effort to bring it up to standard.

The 3-Step Cyclical Maintenance Process

1. Plan for maintenance. If your document is being published for the first time, create a maintenance schedule. Determine how often the document needs to be updated—every month? 6 months? a year? This depends upon the perishability of the information. For example, if the subject about which you are writing is in a contant state of flux, you may have to update the documentation for it fairly frequently.

2. Publish the initial document. If you *plan* for maintenance, you can get the document out where people can use it and, in due course, give you feedback for future revisions. Be sure you *ask* for feedback; set a deadline for it. Keep a log of all the comments you receive, then, when it comes time to perform maintenance on the document, act on what you've been told. Should you receive feedback *after* the deadline, save it for the next maintenance cycle.

3. Create a maintenance guide. This should contain the following:

• a cover page with the title, authors and/or contributors, and any other information that helps to identify your manual;

• a table of contents;

• a brief description of the document—what it's about, what it looks like, etc.;

• maintenance requirements
- maintenance schedule;
- a person responsible for each section (the subject-matter expert, or, if the project has been divided among a number of editors, the editor in charge of each section);
- maintenance process—the detailed plan to bring a particular manual up-to-date;
- location of material—where is it, how to get it, where all the originals (graphics, photos, charts, etc.) are kept, how the material is organized;
- software used to generate the original copy;
- style guidelines (specs, style sheet, a list of your deviations from the original);
- a list of graphics, figures, charts, and tables, and a brief description and the source of each (Note how these elements were incorporated into the document—scanned, drawn, pasted, waxed, or typed in);

- production information: schedule, cost (if applicable), tabs, loose leaf or perfect bound, trim size, cover design/color, paper stock; two- three- or four-color; where printed, number of copies;

- distribution—who gets it and where are they located. (This is important. You need to know your customers' names and addresses in order to send them updated versions, solicit their feedback, and to keep track of how many manuals you have in circulation.)

VI. SOME POINTERS

• Rag right is the most "user friendly" text format; besides preventing "rivers," it also rescues the reader from the rigidity of "boxed in" justified text.

• Rag left is very unusual and can be a most effective attention-grabber if used sparingly.

• For long blocks of text, serif type is still preferred over sans serif.

• Heads, lists, anything not strictly text, are forms of graphic and should be treated as such.

• You must have *some* white space in every graphic.

• Half of a text page should be white space (includes margins, leading, gutters, etc.).

• For more interesting headers, put rules above them. This will make them stand out more. Also, make sure all heads, lists, etc., are consistent throughout your document.

• If you use bullets for lists, make sure that the bullets are 2 points smaller than the text they precede and are centered.

• A line of text on a single column page should run 1½ to 2½ alphabet lengths (40–60 characters depending on the font).

• Use en-dashes (–) for inclusive numbers and em-dashes (—) instead of standard dashes to separate clauses.

• *Never* underline text unless you are typing. Use italic for anything you're emphasizing.

• You may want to consider vertical rules between two or three columns of rag right text. They help to separate columns visually, and they look nice.

• Borders can either be physical, visual elements (rules, for example) or white space. Make sure all rules are proportional to the text they set off.

• While color can make your document look especially sharp, it is very expensive. A workable alternate is to use screening, a relatively inexpensive and simple procedure, that allows you to take one color, black for example, and turn it into gradations of grey. You can thereby have a number of "colors" for the price of one. Colored paper is another way to sneak in additional color.

• When dealing with printers, get samples of something similar that they have done to see how they handle it.

• Non-standard trim sizes are *very* expensive and can cost more to mail. Unless you have a compelling reason for using a non-standard trim size, don't.

VII. THE EXHIBITS

As is usual in professional conferences, various vendors and contractors were present: printing and publication services, translation tools and services, data conversion, editing and design consultants, commercial trainers, university courses in rhetoric. Not surpringly, the printed word is yielding to electronics; CD roms are replacing multi-volume reference books. The GPO is a leader in CDs with maps, statistical information, and other references, from agriculture to zoo. Some vendors had drawings and contests, with rewards ranging from keychains to computers.

The highlight was the exhibit of prizewinning entries in many categories: technical articles, whole publications, brochures, newsletters of small, large, and medium circulation, books, computer documentation, house organs, organizational materials, and so on. From the top down, the four levels are Distinguished, Excellence, Merit, and Achievement. Those of us working on periodicals paid particular attention to the categories Whole Periodicals and Newsletters. The Distinguished were simple in design and easy to read, while Achievement were more cluttered. We paid particular attention to details that characterized the contrasting top and bottom categories.

A concurrent competition was also held for Technical Art. In addition, there was an

audiovisual theater in which the prize-winning entries were shown.

It should be noted that under the aegis of [redacted] *the NSA Newsletter* won an Achievement award in the regional competition of 1985. (*N.B.*: it was submitted, with permission, through channels.)

Special mention must be made of the Online Hit Parade. It consisted of well over a dozen computers, with just about every operating system, including multimedia. Users were invited to test the demos and evaluate them. Among the interesting ones was "Civil War and Reconstruction," a hypercard stack to teach high school students about the civil war. This was designed by Miss Shirley Moore's History Class at the Emma Willard School, Troy, NY.

VIII. A NOTE on PROTOCOL and MORE ADVICE

Exchange of cards is a ritual common to professional societies. Some of us had privately printed cards with our home address and telephone numbers, listing ourselves as "Editor-Writer" or some such. It is advisable to have cards made up--at your own expense--otherwise you may be conspicuous. (The CRYPTOLOG editor can help you on this.) Besides, you might win something in a drawing!

The sessions consist of lectures, panels, workshops, "progressions," (in which you rotate after some minutes) and storyboard talks. A lecture is best if the subject is new to you, while workshops usually require command of terminology and some experience. "Progressions" is suitable for people who are very experienced in the subject. Unstructured panel discussions and storyboarding vary greatly in quality.

The proceedings are mailed to you in advance. We recommend taking that hefty tome with you to help select your choices among the concurrent sessions; you might want to change sessions. Also, we recommend loose-leaf format rather than perfect binding. It's easier to reproduce articles.

We wish that we had thought of taking a camera with us for shots of winning entries. Some people bring tape recorders, as well.

XIX PROFESSIONAL SOCIETIES and JOURNALS for WRITERS, EDITORS, and PRESENTERS of INFORMATION

Society for Technical Communication, 901 N. Stuart Street, Suite 304, Arlington, VA 22203. (703) 522-4114. Individual membership, $85 per year. Includes quarterly issues of the journal *Technical Communications* and 10 issues of the newsletter *Intercom*. There are local chapters in Washington and Baltimore.

Annual meetings are held in major cities in the US and Canada. Future meeetings:

1992 May 10-13, Atlanta
1993 June 6-9, Dallas
1994 May 15-18 Minneapolis
1995 May 7-10 Washington DC
1996 May 5-8 Seattle
1997 May 11-14 Toronto

Another society concerned with presenting information is the National Association of Government Communicators, 669 S. Washington St., Alexandria VA 22314. (703) 519-3902. Annual dues are $65. Includes 10 issues of the magazine *GC*. Local chapters have monthly meetings. It, too, sponsors a competition. Its next conference will be held the second week of January 1993, in Old Town Alexandria.

The *Proceedings* of the 1991 conference may be seen at the A64 Publications Office; Ops 2A 0950. Please call [redacted] at 963-5683 for an appointment to view.

P.L. 86-36

The *Proceedings* of 1988-1991 and other publications of the STC may be consulted at the CRYPTOLOG office, Ops-1, 2N018. Please call the Editor, [redacted] on 963-1103 for an appointment to view.

The *Journal of Technical Writing and Communication* is published quarterly by the Baywood Publishing Company, 26 Austin Ave., P.O. Box 337, Amityville, NY 11701. Annual subscription is $36.00, plus $4.50 per volume in the US and Canada. The executive editor is on the faculty of Rensselaer Polytechnic Institute, Troy, NY. CRYPTOLOG has a sample copy.

From the Past

922

DISPOSITION FORM

SECURITY CLASSIFICATION (If any) C

~~CONFIDENTIAL~~
Modified Handling Authorized

FILE NO.

SUBJECT: Model for Cryptanalytic Technical Reports

TO Distribution FROM: AD/PROD DATE 27 February 56 COMMENT NO. 1

1. The preparation of clear and concise technical reports is an important facet of PROD operations. In technical reporting, clarity and detail are paramount, especially when writing reports on the solution of a new type of cryptosystems encountered for the first time. Such reports should embrace a complete resume of the diagnostic techniques employed in the identification of the system, as well as a comprehensive outline of the steps taken to arrive at the first recoveries of plain text. It goes without saying that close attention should be paid to precise cryptologic terminology in all descriptions of methods and techniques, so as to lessen the chance of ambiguity or possible misunderstanding by the reader. A cryptologic glossary should be freely consulted when the writer is not sure of the exact meaning of a term he is about to use.

2. The attached paper, an extract from the NSA text "Military Cryptanalytics, Part I," is published as recommended reading by, and for the guidance of, all PROD personnel engaged in writing cryptanalytic technical reports. It illustrates what may be considered as a model for such reports. There is no fixed, standard format for these reports because the form and content of each individual report depend on circumstances at the time of writing. However, the attached report on the solution of a hypothetical system is intended to illustrate the amount of detail that might be included.

A. Sinkov
A. SINKOV
Assistant Director
Production

Inclosure
a/s

Distribution: Branch level of
NSA-70 and NSA-90

9221 ~~BDT~~
9222 DW
9223 ~~MW~~
9224 JC file

922 GH
922K CD
~~9 file~~

DD FORM 1 FEB 50 96 REPLACES WME FORM 96, 1 OCT 48, WHICH MAY BE USED.

A copy of the document in question may be obtained from CRYPTOLOG. For a copy write your name, organization, and building, and send it to: CRYPTOLOG, P0541, Ops-1.

Editorial

PERSUMs, TECH TRACKERS, FOR THE USE OF

Now is the time to reconsider the PERSUM.

In his article, "Where are our Textbooks?" (1st Issue 1989) Dave Gaddy decries the lack of technical papers, textbooks, and monographs of recent vintage. They are no longer produced as they once were in the past. Why is that, he asks. And then he speculates on the reasons, and offers a few suggestions.

What he has not taken into consideration, however, is the wording of the instructions in the PERSUM on listing publications. Turn to page 3:

12. PUBLICATIONS (List titles; do not confuse this with reports prepared as a regular part of the job)

Now, at last, we know what really happened. You are not to list reports written as a regular part of your job. So there are no brownie points for writing a working aid, a technical how-to, a reference, a wrap-up report, or the documentation of a technique, as writing them is considered "part of your job." For such papers—when written—are published in an organization's own series, and often, for a limited distribution. They are designed for a specific purpose, for a specific application. They do not fall into the category of general information that would or should appear in a publication such as *The Cryptologic Quarterly* or CRYPTOLOG. Nevertheless, these are the very publications whose absence Dave laments.

So, as the effort is not rewarded, such papers are not written.

Rather, the technical person is better off publishing an unclassified piece, however trivial, in an outside journal: there's far more prestige attached.

Is there a solution? Of course there is.

To encourage the publication of our technical papers, to ensure the continuation of our very own heritage, thus assuring the passing on of the torch, what we should do is to revise #12. It should read:

12. PUBLICATIONS

a. Documentation, working aids, technical how-tos, references, wrap-up reports and monographs prepared as a regular part of the job.

b. Articles in NSA journals.

c. Articles in outside journals.

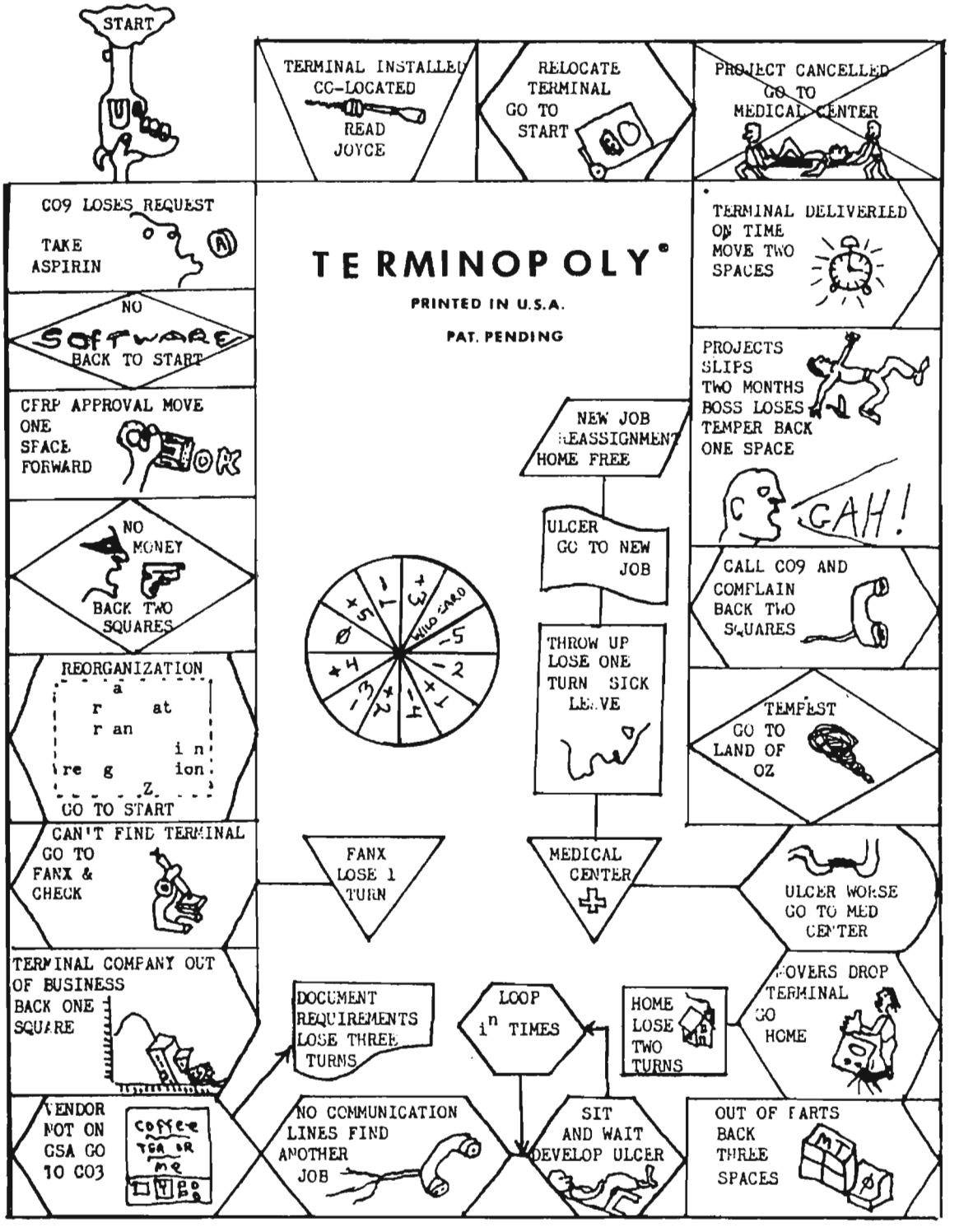
As a columnist recently wrote in the business section of *The Washington Post*, the greatest assets of IBM are its smarts, yet, according to its accountants, its "massive intellectual property holdings are worth less than swamp land in Florida."

This principle applies in NSA as well. We know that our adversaries are moving heaven and earth to get information about our knowledge and techniques. And we know all too well the value, in dollar amounts, they place on specific pieces of information.

But this intellectual property, this knowledge, these techniques, are not held in high regard at NSA.

Reprinted from C-Liners, *Vol. II, No. 3, Issue 13, November 1973*

Golden Oldie



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.

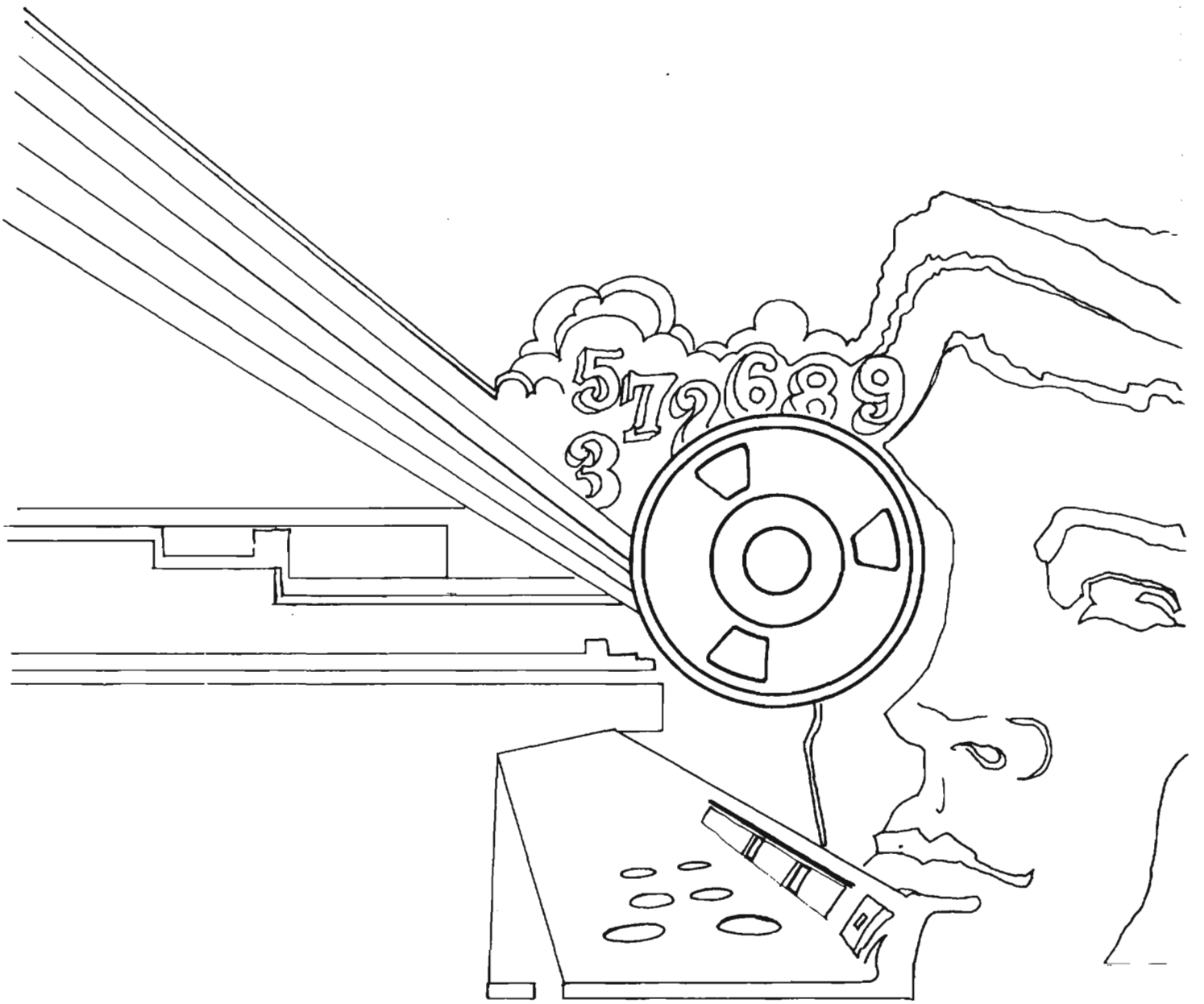
Send two legible hard copies accompanied by a floppy, disk, or cartridge as described below, or use electronic mail. In your electronic medium (floppy, disk, cartridge, or electronic mail) please heed these strictures to avoid extra data prep that will delay publication:

- 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


5 7 2 6 8 9
3