

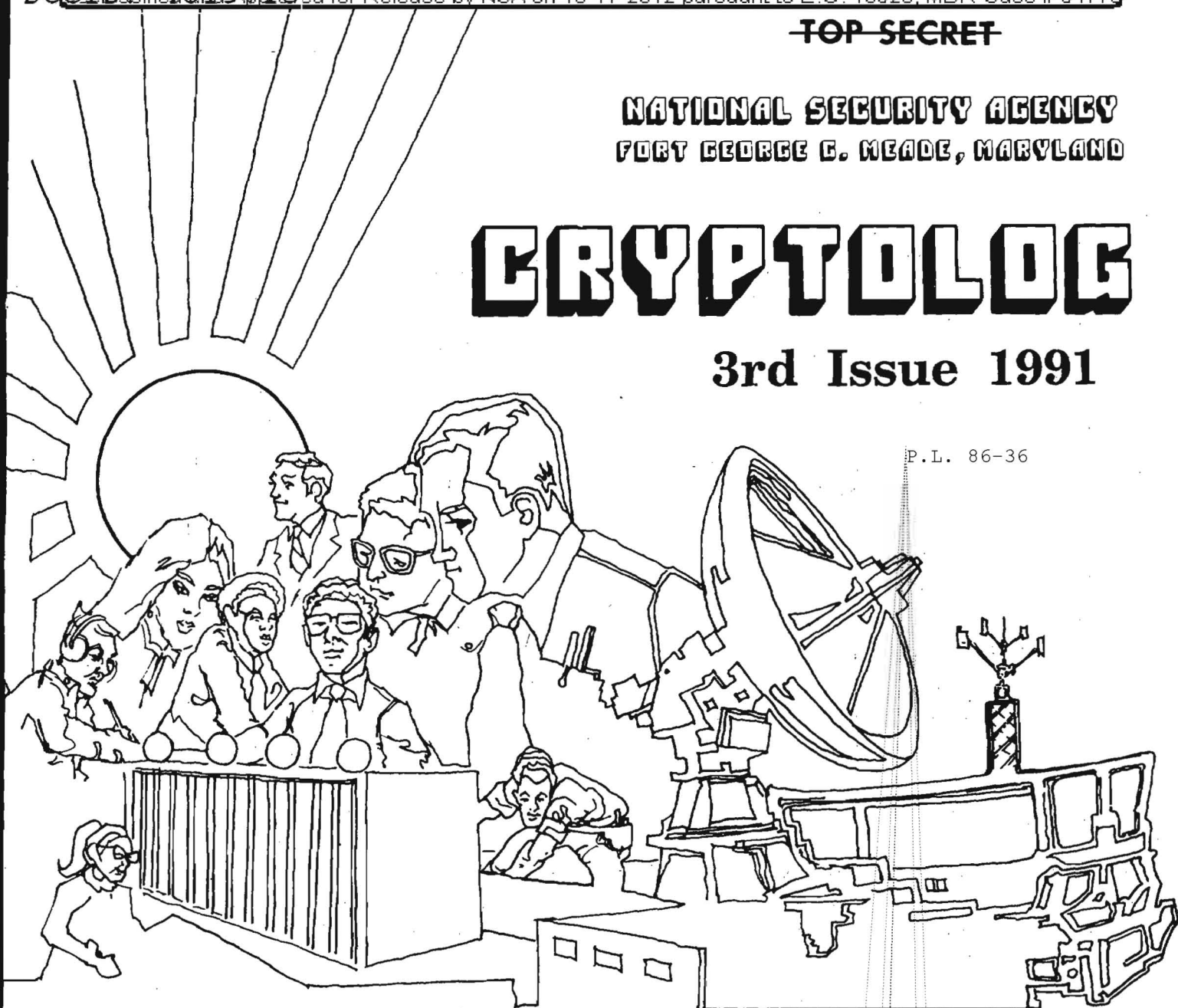
~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

3rd Issue 1991

P.L. 86-36



EDITORIAL	Robert E. Rich	ii
KEYNOTE ADDRESS	[Redacted]	1
FAREWELL TO THE TROOPS	[Redacted]	5
ACHIEVEMENT THROUGH PEOPLE	[Redacted]	8
THE LANGUAGE ANALYST AND AUTOMATION	[Redacted]	13
SIGINT IN AN OPEN SOCIETY	[Redacted]	17
THE WAY IT WAS	[Redacted]	22
A VIEW OF L	Dale Seaberg	31
KEYNOTE ADDRESS	Gerald R. Young	33
FROM THE PAST	[Redacted]	40
ODE TO SIGINT	Al Friendly	41
A MODERN FAIRY STORY	[Redacted]	42
GOLDEN OLDIE	[Redacted]	4, 7
TO CONTRIBUTE	[Redacted]	44

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

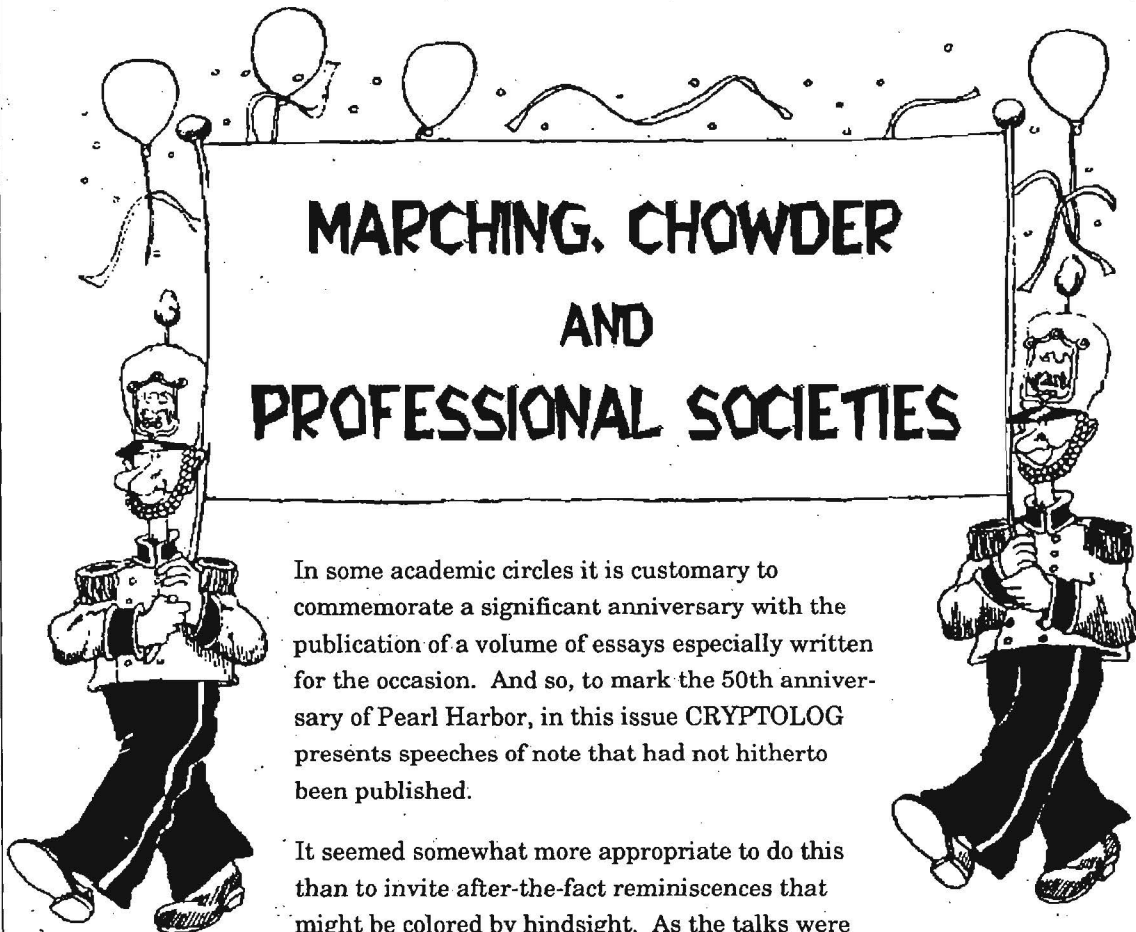
~~TOP SECRET~~

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

~~DECLASSIFY ON: Originating~~

~~Agency's Determination Required~~

~~NOT RELEASABLE TO CONTRACTORS~~

Three Cheers For NSA's

MARCHING, CHOWDER AND PROFESSIONAL SOCIETIES

In some academic circles it is customary to commemorate a significant anniversary with the publication of a volume of essays especially written for the occasion. And so, to mark the 50th anniversary of Pearl Harbor, in this issue CRYPTOLOG presents speeches of note that had not hitherto been published.

It seemed somewhat more appropriate to do this than to invite after-the-fact reminiscences that might be colored by hindsight. As the talks were contemporaneous, they express the actual concerns of the moment. They are snapshots of our past: what we thought was important at the time; what we were worrying about.

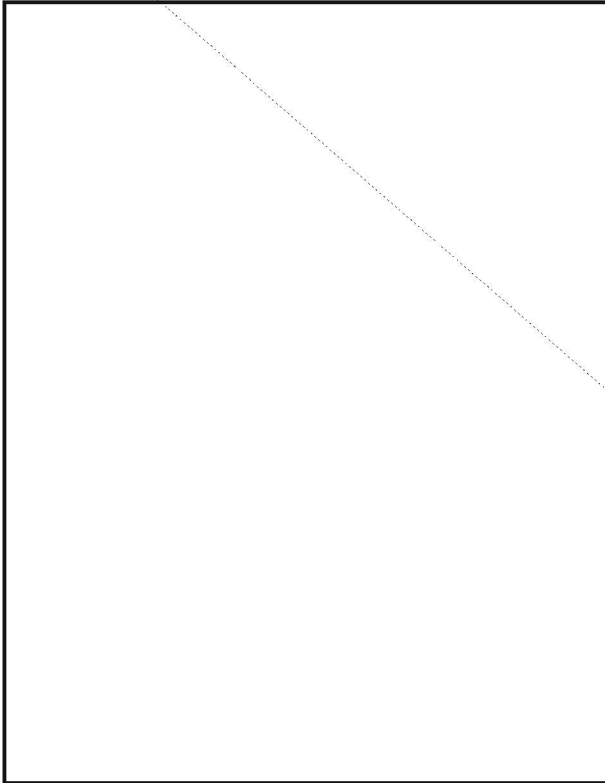
It is interesting to compare the salutatory and valedictory articles; each by a deputy director, to the same audience five years apart. But what five years!

Another custom in academic circles is to dedicate the publication to a worthy party.

Though little known outside the confines of our stronghold, NSA's professional societies play a critical role in disseminating information. To a great extent, the talks, symposia, conferences and seminars they sponsor serve to educate the technical cadres in a manner that formal courses of instruction cannot approximate. Classification permitting, any analyst may attend any talk, whatever the discipline. No requirements! No tests! Just information.

And so this issue of CRYPTOLOG is dedicated to NSA's professional societies.

Long may they flourish!



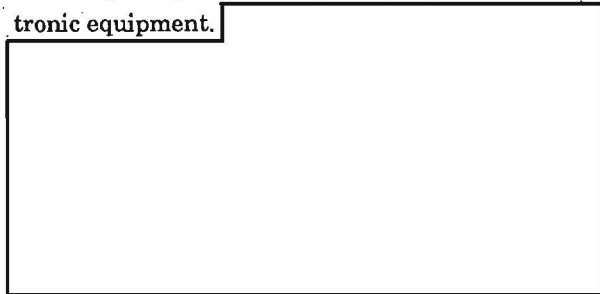
Cryptomathematics Exchange, the Kryptos meetings, and CA-305 are very well attended, and the reports I hear are good.

The [redacted] program, in my opinion, bodes well both for improving the quality of analysis and for contributing to the continued professional growth of our analysts. It will enhance the variety and richness of work experiences that analysts already enjoy and which think is a major factor in the low attrition rate. I would emphasize here that we intend to operate this program intelligently, giving due consideration to the need for continuity on the various problems. I hope that you have noticed that the [redacted] managers have operational backgrounds.

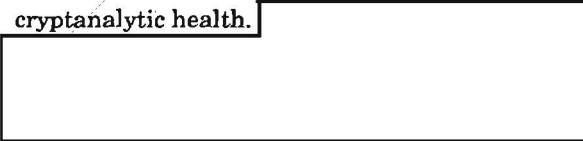
P.L. 86-36

TOOLS

Turning to the tools and systems available for our cryptanalysts' use, it would be difficult to find a more impressive work environment or one better served by computers and special-purpose electronic equipment.



Our relationships with our major cryptanalytic collaborators [redacted] are strong and profitable, and add greatly to the cryptanalytic health.



ORGANIZATIONAL FACTORS

Finally, there are organizational factors which relate to cryptanalytic health. As you know, we are organized principally by target because we think this maximizes synergism. When people talk about functional organization, cryptanalysis is one function often singled out as potentially benefitting. We have repeatedly opted not to change our mainly target orientation but instead, to rely on such cohesion-producers as seminars,

The other kind of CA results, those produced by our COMSEC cryptanalysts, continue to have profound influence on the design of our own cryptologies.

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

THE WORKFORCE

Looking at the cryptanalytic workforce, we find that it has been growing steadily for the past four years at a rate well above the Agency average, and that attrition, especially that due to resignation is very low—less than half of that for the entire Agency—which, by the way, is also remarkably low, about 2.7% for resignations. The CA intern program and the P1 cryptomath program are operating with [redacted] about 70% increase over the number of three or four years ago.

Considering the work environment and the opportunities it offers, it is fair to say that it is good. I see the creation of the technical track and the increased opportunity for reward through promotions and awards to be very positive for your profession. Furthermore, I think that we are doing a reasonably good job in providing for seminars, conferences, and other means of bringing our analysts together for sharing views and problems. Such gatherings as the annual

~~TOP SECRET UMBRA~~

conferences, Kryptos, CMI, CA-305, the math and intern programs, and the panels to promote within-professional contacts.

In addition, at the recommendation of NSAAB the Director appointed a CA Council three years ago which I chair and which serves the functions of high-level advocacy and oversight. For the past three years, we have made an extensive annual review of our cryptanalytic effort for the Director and top Agency leaders. The purpose is to better inform of the progress and state of Agency cryptanalysis. I think these organizational arrangements are close to the best that we can design at this time.

So as not to portray the view that I think everything is roses, I must tell you that some of our cryptanalytic managers believe that our exploitation-research split is out of kilter; that is, we are too exploitation-oriented and are not devoting enough resources to the difficult research problems; much of our success stems from past research successes and our current exploitation may, to an extent, mortgage the future.

I do not totally accept this view, but I do agree that we need to be devoting more effort to difficult unresolved problems and those that we know are coming up in the future. I further think we are making reasonable strides in doing this now. Our research efforts have been strengthened markedly in the past two or three years, particularly in A5, S6, and R5.

LOOKING AHEAD

The rest of this talk concerns the future of our cryptanalytic activity. There is at least one thing we can say with confidence: the long term future ultimately depends on continued success. In my view, the outlook for continued success is good, based on our present posture, knowledge, and momentum. These factors are often forgotten or greatly minimized when prognosticators discuss the future. I want to emphasize them. We have an impressive knowledge base concerning our targets' structures, practices, habits, and systems. It derives from years of study by dedicated analysts and probably one of the most important parts of it is the information our analysts carry around

in their heads. In this connection I want to again mention [redacted] We mean to be sure that [redacted] is run in a way so as to enhance the knowledge base.

But our knowledge and momentum, while exceedingly important, will not alone ensure success in the future. I must hasten to add that there are enormous technical challenges to be dealt with. We must devise very clever ways to obtain solutions using all our "black art," as cryptanalysis once was considered. But with appropriate effort we can deal successfully with sufficient numbers of these challenges to keep our production strong and our own systems secure.

THE CHALLENGES

The major technical factors and trends that must be faced by our Operation analysts are well known to most of you. Basically, they include advances in transmission technology, advances in cryptography, and difficulties resulting from a greater world-wide awareness of cryptography and cryptanalysis. [redacted]

Added to that are the important cryptographic advances stemming from the rapid spread of microprocessor technology and greater use of software-based or more easily changed systems. We are seeing many more new commercial machines and a significant growth in the number of indigenous machines being developed and employed by our targets. Solving these problems will require a dramatic speedup of some of our current methods as well as development of totally new and imaginative techniques.

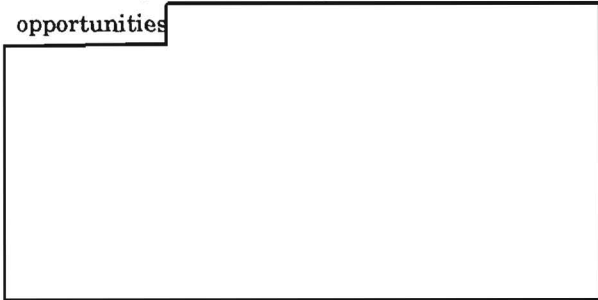
Our COMSEC cryptanalysts have to cope with the growing complexity and rapid development of US civil and military communications systems and the complex crypto requirements related to securing these systems.

Moreover, public awareness of cryptanalytic techniques, the declassification of WW II data and publications about that era, along with the in-

~~TOP SECRET UMBRA~~

crease in non-governmental requirements for cryptography and the attendant public research, have stimulated interest in cryptography and cryptanalysis worldwide and will affect future target cryptography. Another factor affecting the future is the recent strong academic interest, resulting in numerous international conferences and publication of papers on the subject. Operationally, we already see more attention to COMSEC by some of our targets which probably can be traced, at least in part, to the new awareness.

Balanced against these kinds of developments that cause problems for cryptanalysts are many opportunities



Also, of major importance is the fact that our successes have given rise to a general recognition by SIGINT users and government officials of the value of our product and a demand for SIGINT that is difficult to overestimate. The result is powerful support for obtaining the resources we need to do the job.

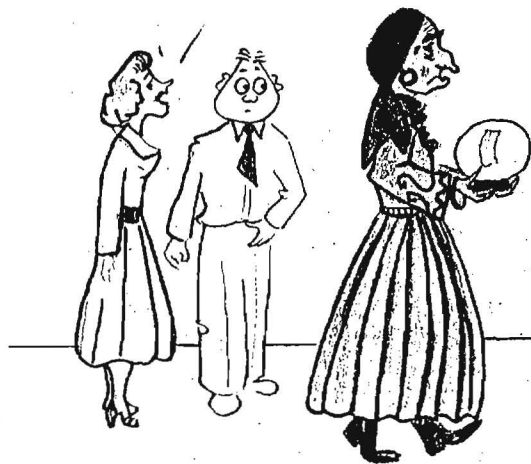
To summarize, I conclude that the health of our cryptanalytic effort is exceedingly good. I am optimistic about the future, but I think we should brace for the challenges to be faced. To help insure future success we intend to continue to pursue objectives that we are already committed to: namely, a broadened research capability; superior development and training opportunities for the workforce; the ability to recruit and hold the best talent available; maintenance of superior tools and processing systems; devotion of sufficient resources and talent to collection, signals processing, and other supporting problem areas; and provision of rewards for technical accomplishment.

P.L. 86-36

Golden Oldie

 c 1955

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



She's cracked TWO systems ALREADY!

scheduling and reporting and concept writing and getting permission to do what their various certificates and job descriptions say they are capable of and paid to do as they spend in creating the actual lessons and tests.

(U) In my view the result of all of this is that first, inadequate attention is being given to NSA's urgent training needs early in the power curve of their emergence.

(U) Second, wrapping the development action in layers of paper loses more time and insulates the developer from the grime, the essence, the reality of the training need. In fact, the whole analysis-development formula reminds me of previous flashes in the managerial plan. Remember PERT? and MBO? Know any place where they are still being used by the people who are doing the work? These techniques are valid but probably only in the specific conditions which spawned them. Their wholesale adoption by a management for different conditions is where the mistakes have been made.

(U) As I said, the current NCS organization is based on a training development formula developed by other people for other conditions. I've no doubt it's valid for those conditions—but for the NCS they are a mistake, a disaster. Well, you're not obliged to accept this mistake any more than my successor is obliged to perpetuate my mistakes. One of the benefits, as well as a prime reason, for changing managers periodically is to provide a graceful opportunity to abandon the previous manager's mistakes. I urge that this opportunity not be allowed to slip away.

(U) The second of the converging problems is the consolidation of all cryptologic training—which seems to have been launched though it hasn't left the ways. I know that we didn't initiate the current action—remove the blocks, to continue the metaphor—and I know, like a genuine launching, it's impossible to stop once started. But then we didn't protest very hard against it, either. Worse yet, for years we didn't attempt to deal realistically or imaginatively with the problem that got Congress upset in the first place: namely, the

rapidly escalating costs of training. We still haven't. Instead, a succession of Commandants have gone in the opposite direction from economical training and have steadily worked at creating a pseudo-college, an institute, complete with deans, curriculum chiefs, learned journals, accreditation, an enormous catalog; in short, all of the trappings and burdens and costs and irrelevance of academia.

(U) Meanwhile, needs here and in the field go unmet or poorly met and contractors grow fat doing system operating and maintenance—even the management—that the Agency is incapable of keeping up with using its own people. For the fact is that building a liberal arts college when we should have been building a trade school—a multilingual trade school, to be sure—has not done much for the real need, namely training in the acquisition, operation, upkeep and management of the galloping technology of SIGINT and COMSEC.

(U) No wonder Congress got frustrated and pressured DoD into consolidation. But that's a mistake too, for the belief in consolidation stems from the myth that one **big** something is more economical and efficient than several **small** somethings. General Motors learned that it isn't necessarily true years ago. Consolidation is a huge red herding, large enough to stock all the delicatessens in the Baltimore-Washington area for a year.

(U) It is a political issue from start to finish. There is no indication that consolidation will materially improve the numbers or quality of cryptologic technical and management people. In fact, the ITRO report did not seriously address quality. And I can accept that, for the ITRO team was, in effect, given a decision to justify. And that's okay too in a political area. The trouble, **the real trouble here**, is that the training arena and the political arena are all under one roof, the NCTS. Thus, it is here that the two problems I identified at the start are in fact converging. And I think that unless that convergence is deflected, O'Brien's law will inexorably take over; our ability to succeed in spite of ourselves will run out.

~~(FOUO)~~ My criticism of the current NCS structure and procedure centers on my belief that the

need is not for formula development of courses or centralized management of training. The urgent need today is to find ways to derive the training directly from, and fit it to, the technology and pressures of the operations. If that is correct, then it follows that training action comes first and political action second. And I say that neither critically or cynically. To the extent that there is a tangible, separate, schoolhouse—to use today's buzz term—is the extent to which we have failed to meet the urgent needs of the cryptologic community. Instead of talking about and planning consolidation of schoolhouses, we should be talking about and planning training outposts, outposts staffed by a Training Corps whose members go out and live in the native villages

[redacted]

[redacted]—not sitting back here endlessly and wistfully planning larger and more elaborate central facilities.

(U) Oh, but you say, be practical, be realistic. Congress has pressured us and the Secretary of Defense has directed us. Okay, I'll be practical and realistic and do so with one recommendation:

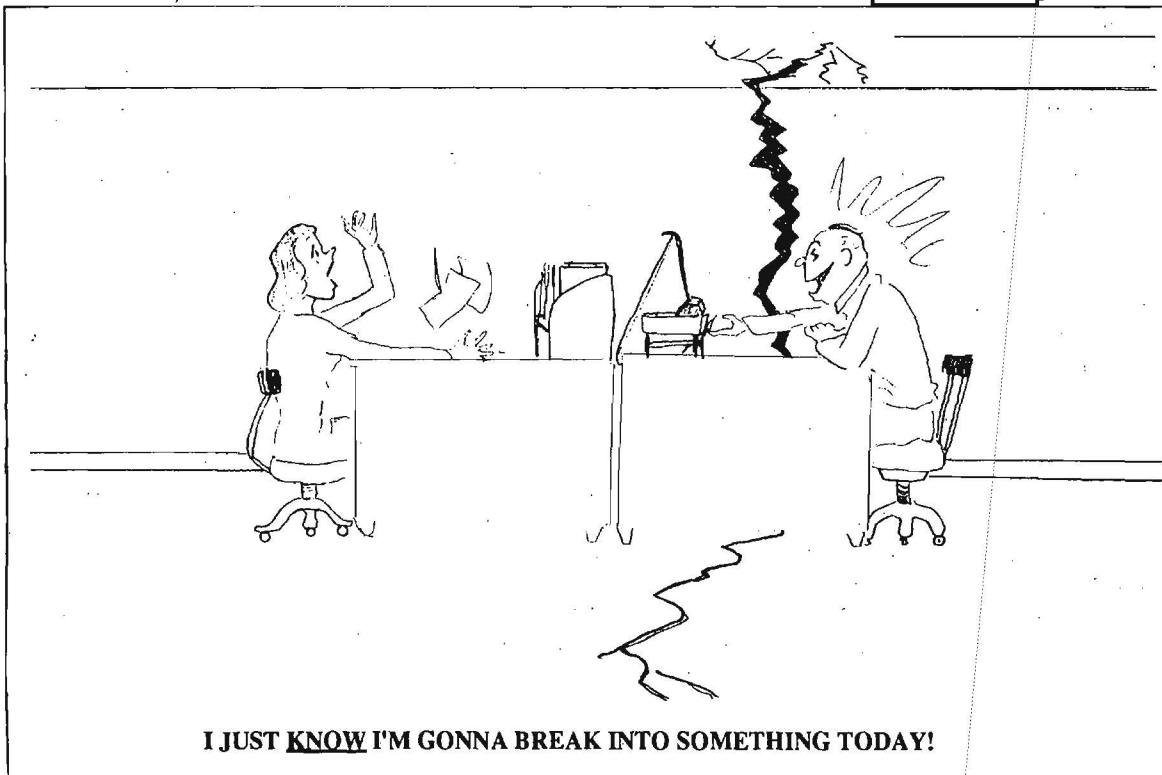
(U) Remove the political activity from the schools and do it somewhere else. Cut the TDNS/CNCS double hat in half. Remove, and I mean **physically**, from the NCS and the Service schools, the small group needed to develop and orchestrate the consolidation plans and actions. Take them, all of them, out of the operational and managerial channels of the schools. Take the political activity and all the attention it demands off the backs of the teachers and developers and requirement analyzers. Give the School—each school—a full-time commandant with the authority and the opportunity to get the training done as his or her first priority. And then reorganize the school part in such a way that it molds itself to the operating needs and not vice versa. Start up the Training Corps and post them out there. A separation of training action and political action could result in both being done better. It puts neither politics nor training in second place.

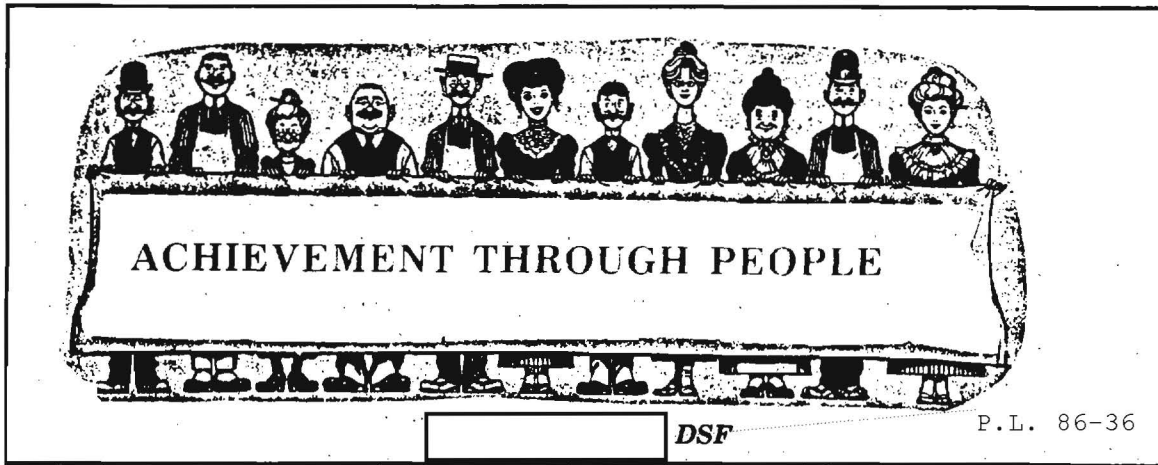
(U) And take it from one who knows full well the price that goes with putting politics in second place.

□

Golden Oldie

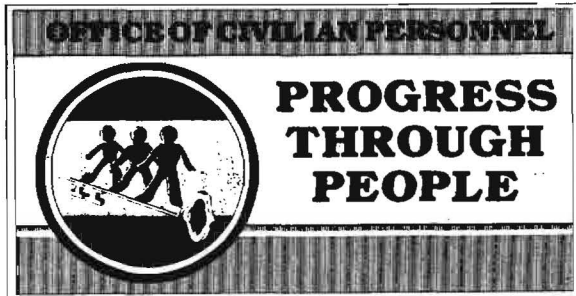
[redacted] 1955





This article is a condensed version of a talk given to the Human Resources Management Association on 27 February 1986. At the time the author was Director, Civilian Personnel, Chief, M3.

"Achievement Through People" -- this is the goal of every organization and every manager everywhere. No one can achieve an organization's mission without people. People are the most important resource, the key, as our M3 logo shows:



This logo was designed by a person in M3 as part of our 5-Year Plan, which I'll describe later. One of the Task Groups under that plan held a logo design contest and the winning one has become our official M3 logo. We use it everywhere: on posters, awards, all printed publications.

The word "Management" means achievement through people. The task that every manager faces is to find the best way to use this precious resource to accomplish the mission. In this paper I am going to talk a bit about management and what my philosophy is; show specific examples of some creative things we are doing in M3, and conclude by telling you how we are doing--where we've succeeded and where we still have a way to go.

MANAGEMENT PHILOSOPHY

Obviously there are many ways to manage people. One's management style is very individual, a blend of one's personality, energies, interests, enthusiasms and skills. It is also a product of what you yourself have experienced under different managers. In my own case, I have always had a lot of ideas. From the day I came to work here I have always wanted to contribute those ideas to help solve problems and to improve the way we do things. Sometimes I could, but sometimes I couldn't. It depended a lot on the management style of the person I worked for. So my own experience influenced my management style.

The climate, culture and traditions of an organization are also important. What do employees expect on the basis of their experiences? This last item is particularly important and particularly tough. When you want to change an organization, you really want to change its culture and that's difficult to do. Some employees cannot accept change; they are comfortable with the status quo perhaps. And there is risk involved for them and for you; some may not be willing to take those risks. Others may not support your goals; you simply may not win them over no matter how hard you try. You may want to encourage innovation, candor, speaking out, but the existing culture may be one where innovation has not been particularly encouraged, where speaking out was frowned on. Thus, new ideas may not be readily accepted.

So it is important to lay the proper groundwork and then work to effect change through education, persuasion and leadership. You must also demonstrate that you are sincere in wanting candor, ideas and help. You must

reward, not punish, for these things. You must be willing to tell the bad with the good; you must also be willing to hear the bad along with the good. It is crucial to get people to trust you.

One of my first initiatives as the new Chief of M3 fell flat because I jumped into it too fast: Town Meetings. I believe communicating with all employees. So I began to hold quarterly Town Meetings in 3 locations: Headquarters, FANX and Airport Square. But they did not turn out as I'd hoped. Some said I didn't tell them anything they didn't already know. Others didn't believe what I said, especially in the Question and Answer period. I was being honest but some did not think so.

Whatever the reason, my timing was off. I had not laid the proper groundwork. So I stopped having Town Meetings. It is interesting that now, a couple of years later, I am getting requests to do them again. People say they miss them. I see this as evidence that the culture is changing.

This is a problem that all creative managers face: they risk not being understood or appreciated by their peers, their subordinates or their bosses. It takes real courage and some sacrifice to persist.

CREATIVE MANAGEMENT IN M3

My philosophy of management is to try to take advantage of people's skills and abilities by **involving employees and having them participate** as much as possible in helping execute our mission. I want to challenge them, to help them be more creative, able to contribute more and be more productive. I believe that **communication** is vital to this process, as is **providing the tools needed to do the job and to grow**, such as training and modern technology. I think it is important to say thank you by giving **awards** for doing a good job. And it's important to remember to stop now and then to have **some fun** together. I'm going to discuss these five topics, leaving the first until last because I have the most to say about it.

The most striking feature of M3 is its geographical dispersion.

Some of us are centralized at Airport Square 1 but the rest are all over the place. This decentralization is intentional. The IPA concept (the decentralized units are called Integrated Personnel Activities) is built on the idea that

we need to be close to the people we serve. While it all works very well for that purpose, it does make managing M3 much more difficult. The fact that the IPAs have 2 masters--the Key Component and Group Chiefs they serve and M3--and that we are geographically dispersed sometimes creates a "we" and "they" atmosphere. One final note -- when I joined M3 in January 1982, I was the third Director of Personnel in just four years. This means that the change of direction and leadership happens frequently in M3. And the Director has always been someone from outside the organization.

COMMUNICATION

I place a very high priority on telling people what they need to know to do their jobs. Let me give a few examples.

We have an electronic mail system on our computer called COMET. We use it constantly throughout our geographically scattered organization for all sorts of quick communications. We announce M3 assignments, reassignments, promotions and training opportunities. We advertise internal vacancies and use it to distribute minutes of DDA staff meetings. This, by the way, is one of my innovations that people do like. And distributing staff meeting minutes on COMET insures that everyone gets a chance to see them.

Once a month we hold a **monthly program review**. Anyone in the organization who wants to attend is invited; it is not meant just for certain higher grades or just for the managers. The idea is to give all the people in M3 the chance to broaden their knowledge about things going on throughout the organization and the Agency. We review budget, policy, resources, the status of major programs and reports on our 5-Year Plan.

Our biggest problem is finding a room at FANX large enough to hold our MPR. Recently I started to hold a mini-Town Meeting as the first 15 minutes of the MPR, giving news of interest and then answering questions.

We publish an **annual report** on M3. It is no ordinary report as you can tell from the index: "Welcome Aboard" tells about our hiring program; "On The Front Line" describes activities in our IPA's; "It Pays to Advertise" is about our Competitive Selection Program; and "More Cold Cash" reports on our Awards Program. We all look back with pride on the year's accomplishments. And we circulate the

report to a wide readership, including the Director and Deputy Director of NSA as well as DDA.

Every so often we have an informal give-and-take around our conference table with DDA and A/DDA. We call it a **rap session** and all my Division and Staff Chiefs as well as a representative from the IPA Chiefs attend. This allows us to talk together about anything that's on our minds. We can discuss hard issues, or things we just need to understand better. The chance for all of us to do this face-to-face and directly with senior management rather than my bringing it back to my managers secondhand has been extremely helpful, especially when discussing policy and philosophy. After we finish the RAP session, we all go out to lunch together.

I believe that **giving the tools needed to do the job and for personal development go hand in hand.** The more people learn, the better they can do their jobs. I have really emphasized this in M3 in all aspects: education and training, professionalization and cross-development.

We encourage people in M3 to become active in developing themselves and have designed an **annual assignment questionnaire** for them to use for this purpose. Anyone who wants to can complete and return it. We use the information to help plan the moves of M3 people for diversity, for professionalization, a move from technical to management or vice versa, and an opportunity for cross development. In the first year, almost all those who returned it got one of their choices for a different assignment.

EDUCATION

My emphasis on **education** has finally paid off. In just 4 years, we have greatly increased the number of people in M3 with higher education. In fact, M3 has now surpassed the NSA average in numbers of people with college degrees. This was not easy to do, and it took a corporate decision and commitment of all my managers to pull it off. We do not get new billets in M3, but we agreed that whenever we did get an empty one we would hire or bring someone into M3 who had training in our preferred fields of interest. We now have a large number of well qualified new people in M3 and the results are what you have seen.

I have high regard for my on-board employees as well; they have also responded magnificently to the challenge to develop themselves. 54 of

them are in college now, including many of our clericals. I am especially pleased at that. Those not able to pursue college are using opportunities for training at NCS and OPM. We have also arranged to hold special OPM courses and some college courses here at NSA for our M3 people, so larger numbers of them can attend.

We have set up a special program called a **staffing plan** to train and develop all the new people we have recently brought into M3. It's like an internal intern program. The idea is to make sure people start out right and learn all the things they need to know to serve this Agency's personnel needs into the next century.

PROFESSIONALIZATION

One area that is still somewhat disappointing is **professionalization.**

Our many new hires have not yet been here long enough to become professionalized. But a lot of our middle-grade people (grade 12 especially) have still not gotten professionalized. We have encouraged these people, but the results are disappointing.

The NCS has created several courses especially for M3, including a tailored one-day version of "Time Management" and a brand new course on "Creativity." Again, everyone in M3 had an opportunity to attend these courses; they were not limited to managers, to certain grade levels or COSCs.

I have had some criticism for my emphasis on education, in part, at least, it is because it is different from the past. But I have persisted and my managers have supported me. The results clearly show success. M3 is hiring very high quality people for all the rest of the Agency; we feel that we must do the same for M3. This is yet another example of a change in culture.

AWARDS

One of my most pleasant duties is to be able to say **thank you** for jobs well done--to give our **awards.** I have established two new awards just for M3 so I can express my personal gratitude to the M3 people. One is the Director of Personnel Award. It is a plaque accompanied by a check. I have given out only two of these so far: to [redacted] Chief, M3G, and to [redacted] M33. Just recently we had designed and printed a Director of Personnel

Certificate which I will be awarding in the future.

Our **monthly award ceremony** is a special event in M3. I always conduct this ceremony myself. I want to give wide visibility to the things M3 people have done and let them have some well-deserved glory. The photographer says he likes to come to our ceremonies because they are so interesting and so much fun.

FUN

Speaking of **fun**, we feel we just have to stop now and then and enjoy ourselves and each other. Our **Christmas open house** has become a traditional annual event. Everyone pitches in to cook and bake tasty and beautiful foods for our all day buffet. We set up the spread in our conference room and invite everyone, from all the far flung areas of M3, to stop by to visit, talk and have some goodies. I enjoy this once a year chance to see almost everyone in M3 and to chat personally with them.

One of our most successful pleasure activities was a combination of work and play. The Image Task Group under our 5-Year Plan came up with the idea for an **image seminar**. They felt that M3 is a service organization, that we have a public face and can improve it. We invited every single person in M3 to attend: all grades, all skills, military and civilian. I was told: "Virginia, You can't shut down M3 for a day." I said: "Just watch me." It was so important to me that everyone come because everyone is important to the M3 mission and I wanted them to know that. We heard an outside speaker tell us how to deal with the public and each other. She gave the seminar twice that day, once in the morning to half of us and again in the afternoon to the rest. But the highlight was the luncheon--we had everyone together for that. It was the first time ever that all of M3 had been in the same room together. People met other people who had been only phone voices to them.

We had a lot of fun over Christmas with a new idea--a **pet show**. Actually it was a **PET picture show**. The pictures were judged and prizes were awarded in a ceremony. There were carrots for the rabbits and horses, catnip for the cats and bones for the dogs.

INVOLVING EMPLOYEES

Two of my most important objectives fall into this category. I consider them the bases on which everything else builds and depends.

First, I wanted to **build teams**. I did not want independent fiefdoms of Divisions, Staffs and IPA's. Secondly, I wanted to provide chances for **wide employee participation**. I believe that everyone has good ideas, whatever one's grade level or position in the organization. The problem is--how do you tap all that talent, creativity, ability? Well, here are some of the things we have done in M3.

We use our **M3 staff meetings** primarily to **solve real problems**. We do, of course, exchange information as is traditional in such meetings.

We set out deliberately to build some teams. The first one we established was our **career management board**, informally called our People Meeting. All our Senior managers (Division and Staff Chiefs) sit on that Board and they put on their M3 hats to handle all internal staffing for M3: reassignments, rotations, reassimilation and developmental assignments. They also meet as our M3 promotion board. The results of their deliberations are then made as recommendations to me. It was hard at first to break old patterns; the instinct to look out for number one first is very strong. But I have been very pleased at the ability of the M3 managers to look at the overall good of M3 and the Agency.

We have had a number of formal **team builds** on specific topics. The M3 managers and the IPA Chiefs recently met to discuss the inevitable problems created by being so geographically dispersed. Personal contact is not very frequent and it generates lots of misunderstandings. We felt that the "We" and "They" problem needed to be discussed. After it was over, we agreed that this was one of the best experiences we've ever had--our critique scores were exceptionally high. Note, however, that we had been working together for several years before we did this. We had built the climate and culture for it. It probably would have gone the way of Town Meetings had we tried it earlier.

The Team Build idea has percolated through the whole M3 organization. We have had successful team builds for the M3 Training Coordinators, the M3 Classifiers, the M Secretaries and the Country Desk Officers in Field Support. Every single team build has resulted in lists of solutions to problems and new ideas to try.

Our most successful initiative has been our **M3 5-year plan**. We have done this for three years

now and always done it wholly in a participative environment with broad representation from throughout M3. HRMA, the newest professional organization (Human Resources Management Association) at NSA, started out as an idea in our 5-Year Plan. I put it up during the brainstorming and the whole group bought the idea. The GOODIE Task Force is starting Quality Circles in M3.

The RAP Task Group started program evaluation for us. We have not had any billets for years for this important function. But the 5-Year Plan collected some volunteers from all over M3 willing to help us get it started. They have now all attended a formal training course, and are busy evaluating the Competitive Selection Program. It's another example of doing more with the same--of increased productivity.

The AUTOMAN Task Force is automating the PMM (Personnel Management Manual) with the goal of making it available through remote access throughout the Agency eventually.

TWOTEN and PROSPECT got a small personnel research effort started. Again, we have had no billets for a long time for this important function. And, again, we have done it anyway using volunteers and by increasing productivity. Their first publication in our new series "Issues of the Eighties" is entitled "Comparable Worth." The SOS Task Force, or Secretaries on the Spot, are studying how we might set up a Kelly Girl type program at NSA. The group is composed mostly of M3 secretaries.

HOW ARE WE DOING?

The last thing I want to discuss is: "how are we doing?" I might not have had a very good feel for this if it weren't for still another 5-Year Plan Task Group called ENTERPRISE. This group interviewed and surveyed a sampling of the M3 work force to find out.

How are we doing interview questions

1. What steps could you take to become a more effective employee? How could your co-workers help you to do your job better? What could management do to enable you to be more effective in your job?
2. If I were your supervisor, what suggestions would you have for me that would enable your work group to become innovative?

3. Describe how your immediate supervisor encourages airing of problems, concerns, or differences of opinions.

4. How are suggestions to change plans, procedures, or goals reacted to and handled by your supervisor? Give examples.

5. What suggestions can you make for M3 management that would encourage creativity in the "rank and file?"

6. What suggestions do you have for M3 management that might improve their own effectiveness and creativity?

Other comments.

I can't tell you how wonderful it is to have this kind of information directly from the people. I've learned some really helpful things. I've been pleased to find out that, on the whole, things are going very well indeed. Everyone in M3 seems to know about and to like the 5 Year Plan. And they also know about and like the emphasis on creativity, innovativeness and the chance to participate in the Task Groups and the Quality Circles.

My interest in sharing information may not have penetrated as far down through the organization as I'd like. Also my goals may not always be interpreted and reported as accurately as I'd like. The communications problem again! For example, everyone says we need more resources. I know that, of course, but apparently my people don't know that I know.

I also learned that I must talk directly to my people more often. So I am starting RAP sessions every month with small groups of employees, a different group each month.

So, I find that things are going well. I am blessed with a wonderful Deputy, a super group of senior managers (Division, Staff and IPA chiefs), and a very capable, dedicated and loyal group of employees throughout the organization. I'll end with a few words of encouragement from my people. One said that in all the many years she has been working, mostly outside NSA, she has never before felt such freedom to use her talents and do things to contribute to her organization. They show me that there are many people in the work force who are eager to try something new and different. They like what I am trying to do and are encouraging me to keep at it. And I will.

~~SECRET~~

a consumer representative that the translation is not yet ready even though they have had the message for ten minutes already-

[Redacted]

when our language analysts had finished, then another language analyst called a checker reviewed all these jobs, assuring that the product represented a faithful rendering of the original, that all addressees had been included, and that the language analysts who did the product gets adequate feedback.

~~(S-CCO)~~ The voice world differs in a number of ways, but is no less exacting: the language analyst who is a transcriber mounts tapes, listens to them for content, engages in the same kind of research to determine the who, what, when, where, and why of the traffic,

[Redacted]

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

COMPUTER SUPPORT

~~(S-CCO)~~ If that is what language analysts do, what support does the computer provide? Here are just a few examples:

- For support to bookbreakers, we have

[Redacted]

P.L. 86-36

- For message separation and distribution programs there have been

[Redacted]

- Word lookup was provided to the Chinese language analysts via

[Redacted]

- In Russian and a number of other languages, reverse dictionaries were cre-

ated, to help the language analysts struggling with a garble.

- In Vietnamese, dictionaries were sorted on the second and third syllable, for the same purpose.

[Redacted]

- Indexes of English-to-Russian dictionaries were created, as a means of getting back to the English from the Russian.

- Large "dictionaries" were created, beginning with the Spanish-to-English CAMINO system and expanding to many other languages.

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

[Redacted]

[Redacted]

- For Information Retrieval, [Redacted] [Redacted] were developed to facilitate searches through raw traffic and end product.

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

- Remember the Farrington Optical Character Reader? The Kurzweil Data Entry

~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

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

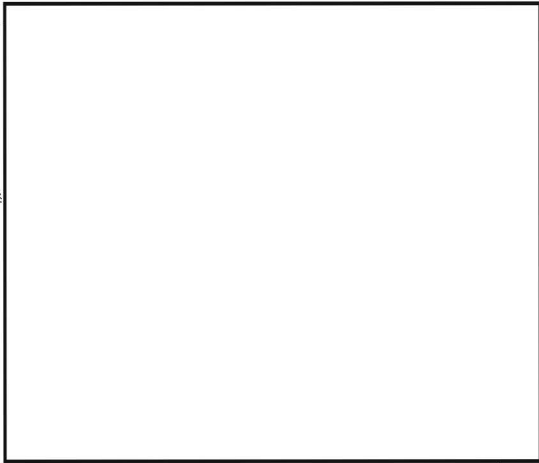
P.L. 86-36

~~SECRET~~

Machine is the recent version of such a scanner.

P.L. 86-36

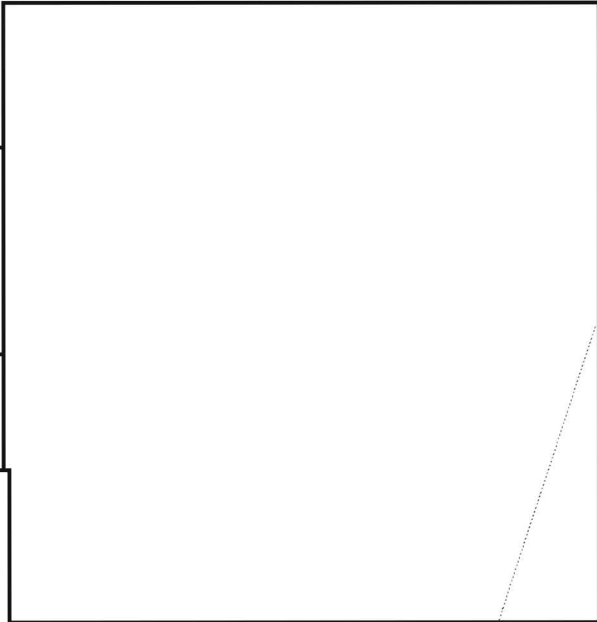
- A lot of these programs—or their successors—are still going strong. [redacted] probably merits some kind of longevity award.



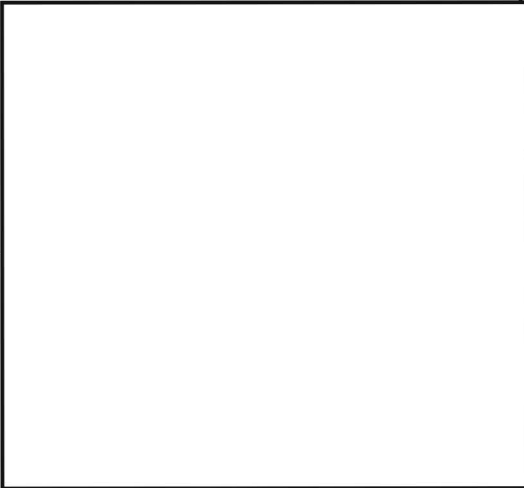
- There are now dictionary files in the CAMINO format and other format in several languages.
- High quality printing of the scripts is available through use of the SEACO 1700, which produced a hard copy of the Turcofile. For the English, variable-width characters may be selected, and both right and left margins may be justified.
- The same is true of the Russian-to-English Glossary [redacted]

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

~~(FOUO)~~ Transcribers have not been forgotten in this process: we have a terminal for data entry, complete with some text editing or word processing capabilities. Eventually the transcriber should be able to access a variety of files from this terminal as well. The analog tape will be replaced by a digitization procedure, making it possible to skip most of the silent portions and have great power in selecting the next cut to process.



~~(S-CCO)~~ That's all well and good, you say, but what can a computer do with garbles?



WHAT'S BEEN HAPPENING IN THE REST OF THE WORLD?

~~(FOUO)~~ If I were to name the single biggest contribution of technology to the NSA language analyst during the 1970's, it would probably be the widespread development of language files on computer tape. Much the same sort of thing was happening in many other parts of the world. Gov-

~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

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

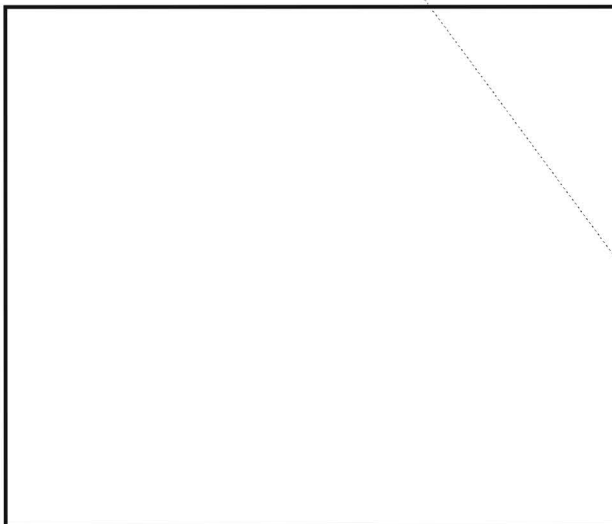
P.L. 86-36

~~SECRET~~

ernments and industrial firms alike became immersed in developing adequate lexical support to translators, in this age of rapidly advancing technology and hence rapidly changing terminology. In Canada, Holland, the Federal Republic of Germany, and the European Economic Community a variety of terminology banks were designed and developed. An organization called INFOTERM assumed the task of coordinating these various term banks.

terminals will become commonplace. The language files developed during the 60's and 70's will be made available to NSA language analysts via the terminal, as will those information files so prevalent today. But another development will be various kinds of machine-aided translation.

(U) Another notable occurrence during the 70's was the widespread adoption of dictation equipment to speed the work of the translator. The translator reads the translation into a dictating machine, and the tape is then transcribed by a specially trained clerical person known as a transcriptionist. At the UN and many other places, transcription is the preferred method of rendering a translation.



WHAT'S AHEAD IN THE 1980s?

~~(FOUO)~~ I believe that the big news in the decade ahead for the language analysts at NSA, as well as for the translator at large, will be the widespread use of interactive terminals to provide various kinds of programming support.

~~(FOUO)~~ Their philosophies may differ slightly, but the message is much the same—the ubiquitous computer terminal has much to offer the translator, the transcriber, the lexicographer, the terminologist, and, yes, NSA's language analyst. Just to prove it, I'll point out that this presentation was prepared with the aid of

~~(FOUO)~~ Some analysts at NSA already use terminals for data entry, for receipt of materials and/or for information retrieval. In the years ahead,

prepared with the aid of
prepared with the aid of

a terminal attached to an NSA system called

And it came out just fine.

P.L. 86-36

Notice to Contributors

Please note the new mailing address

OPS-1, P054, CRYPTOLOG

Look carefully on the box or disk before you format your disk.

If you are using a 5 1/4 disk, see whether it is HD or DD. If it is HD, do not format it as DD. It will not read. It must be formatted as HD.

If you are using a 3 1/2 Mac disk that is 1.44 mg, it must be formatted as HD.

**Remember to label your floppy with the following information:
Your last name, organization, building, secure telephone number**

~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

Secrecy in an Open Society



James Martin

This is a condensed version of a talk given at the Business Luncheon Series on 21 January 1987. At the time the author was a staff member of the Senate Select Committee on Intelligence.

Let me give you a little background on exactly what I do for the Senate Intelligence Committee. I'm the number two budget officer and, as such, unlike some of the other professional members of the staff, I'm not tied to any one particular senator on the committee. We have fifteen senators on the committee and each one has one member of the staff who, in effect, works for that senator. Then there are a few members of the staff which are core professionals who work for the committee as a whole. I'm one of those core professionals.

What that means is that I scrupulously avoid being at all partisan in my work. I serve the Democrats and Republicans equally. That's really not too difficult since our committee is not nearly as partisan as most committees on Capitol Hill. The members of our committee take their oversight responsibilities very seriously and recognize that the sensitive nature of the information we handle makes it imperative that the committee operate in a bipartisan or non-partisan manner. That being said, you have to recognize that the United

States Senate is a political organization, and it would be naive of me to try to convince you that politics does not sometimes intrude on the business of the committee. It does and that's just a fact of life.

But, I can assure you that our committee, senators and staff, strives to deal with the issues from the perspective of what is in the best interest of the National Security of the United States. I had breakfast last week at the Pentagon with General Peroots, the head of DIA, and he told me that Senator Byrd, and the new Majority Leader of the Senate, asked him for his advice as to how he should handle the Iran/Contra investigation. General Peroots told him to be a patriot--be an American. I know it sounds corny, but that is really how we try to approach our oversight responsibilities. We get sidetracked from time to time, but on the whole I think we do a pretty good job of avoiding the political pitfalls.

Specifically, what I do for the committee is to review the budget requests of different elements of the Intelligence Community including, among others, NSA. I plow through the myriad of documents, books, briefings, etc., which in excruciating detail explains what General Odom proposes to do with the budget that the President is requesting for him. That's the easy part. Then I have to boil it all down to a brief,

coherent and understandable for the senators who, of course, make the final decisions. And remember, senators are extremely busy people and this material is very technical and confusing even for someone who deals with it all the time.

Of course, I don't spend all my time reading budget material and briefing senators. In order to really comprehend how all of the various components of US Intelligence operate, I do get out from time to time to "kick the tires" so to speak. Since joining the committee staff, I have been fortunate enough to visit Moscow twice, England and Germany twice, Australia, California, Colorado, and several other nice and some not-so-nice locations. And then there are activities which develop on an ad hoc basis which demand my time and attention. The current situation involving the Iran/Contra affair is a prime example of this.

When Minnie Kenny first mentioned the series of lunches and asked me to speak at one, I was both flattered and surprised. I wondered why 150 people would want to pay \$8.50 to eat lunch and hear me talk. After I finish you may be wondering the same thing. But, in any event, I thought it would be fun and I said sure, why not?

What should I talk about? I doubted whether I could hold anyone's attention describing such aspects of the congressional budget process as the difference between an authorizing committee and an appropriating committee, or the effect budget authority versus budget outlays have on calculating the amount to be sequestered under the Balanced Budget Act of 1986--otherwise known as Gramm-Rudman-Hollings.

I decided to talk about "secrecy in an open society" for many reasons, not the least of which was that it might stir up some interest and perhaps some skepticism on the part of people who might attend the lunch. My goal is not to lecture--or to titillate for that matter. What I hope to do is to give you some food for thought on the subject--to give you some opinions I have on the issue and, more importantly, to stimulate discussion.

My fifteen months with the committee have been anything but dull. I am reminded on the proverbial Chinese curse: "May you live in interesting times." Well, we in the intelligence business certainly live in interesting times! 1985 will long be remembered as the "Year Of The Spy" with this discovery of the Walker

family spy ring; the arrest on espionage charges of a former colleague of yours, Ronald Pelton; the defection/redefection of Vitaly Yurchenko; and the Jonathan Pollard/Israeli Capar.

THE YEAR of the LEAK

1986 may well be known as the "Year of the Leak." We were bombarded with headlines based on leaked information such as: "U.S. discloses secret plan by the Sandinistas"; "CIA Anti-Quaddafi plan backed". And, of course, there was the role of the media itself in reporting leaks and in how it should cover spy trials. I'm sure you remember the controversy involving Bill Casey, General Odom, and *Washington Post* editor Ben Bradlee over what information the Post could use in its coverage of the Pelton trial. Whether you agree with Casey/Odom or Bradlee and the Post, I'm sure your opinions were strongly held.

And finally, in 1986, in case you have been travelling in a remote and inaccessible part of the world, we have the current situation involving the arms sales to Iran and possible diversion of funds to the Contras.

We're going through another round of leaks now which raise several questions. I cringe these days whenever I pick up my *Washington Post*. Just two Sundays ago, for example, you good folks were prominently featured in the headline for the lead story. I know it is troubling for you and I can assure you the committee is frustrated and disturbed by the developments of the past few weeks.

I guess I'm still naive enough to think that secrets given in a closed session in a secure facility would remain secret--at least for a day. So you can imagine how I felt a few weeks ago when, after a long day at the committee during which Robert McFarlane testified before our committee, driving home about 10 p.m. I heard the lead story on WTOP, "former National Security Adviser Robert McFarlane, in secret testimony before the Senate Intelligence Committee today, detailed his role in the etc., etc., etc." I about went off the road. It was just the beginning of a long series of similar occurrences.

That being said, I would like now to throw out a few thoughts on the nature of secrecy in this country and the climate in which we all have to operate. In a recent essay entitled, When Secrecy Meets Democracy, *Time* magazine posed the question, "Can Americans do anything in secret anymore?" The essay points out that one

consequence of the arms for Iran story would be an unravelling of an endless series of disclosures--names, dates, places, faces, etc., that will make it very unsafe to be an American agent: remember this was written back in early December. As we now know, that is precisely what has happened.

In the early 80's, Israel had, then lost, contacts in the middle levels of the Iranian military. They died out according to an Israeli official. He told the *New York Times* that the contacts were executed. There was also a recent series of stories in the press about a number of KGB agents who were executed in Iran after their identities were made known to Khomeini. The premise of the *Time* essay is that Americans are passionately democratic, and thus acutely sensitive to the contradiction between democracy--which promises openness--and the secret world of diplomatic and paramilitary intrigue. Americans do not take easily to the notion, for reasons of state, secrecy may sometimes be necessary. We have only to look back to 1929 when Secretary of State Stimson found out about American code-breaking and interception operations and stopped them with those famous words I'm sure you're all familiar with, "Gentlemen do not read each other's mail."

Since then we have had another world war, the cold war, and now "low-intensity conflicts." According to *Time*, the first of these spawned to OSS, the second gave us the CIA, and the third produces everything from the Delta Force to Ollie North and the cowboys at the NSC.

So what does all this tell us about the climate in which we find ourselves today? Certainly I'm preaching to the choir, and by the way I consider myself to be an active member of that choir, to say that there is a legitimate need to conduct certain sensitive government operations in secrecy and that some information, because of the harm its disclosure would do to National Security, must be protected as classified information.

PROTECTING THE "REAL" SECRETS

By the way, I strongly believe that one of the things we are going to have to do is to sharply limit the amount of information that we protect as classified. There is an old saying which says, "He who seeks to protect everything, protects nothing." I believe that. Some of the information we try to protect today just does not stand up to the supposition that its

disclosure could harm the National Security. We simply do not have the resources to protect everything--nor should we try. Obviously I can't give you any examples in an open session, of classified information which shouldn't continue to be classified--either because it just doesn't meet the standard or because it is already common knowledge. The Stillwell Commission, which was set up after the disclosures of the Walker case, concluded the same thing and has recommended sharply limiting the amount of information the government classifies.

We need to protect the "real secrets." Another point I want to make regarding secrecy is that, while it is potentially a breeding ground for lawlessness, it is also a breeding ground for genius. Without secrecy, we wouldn't have had Henry Kissinger's secret trips to China or the most recent interception of the hijackers of the *Achille Lauro*--an idea, by the way, that most people attribute to none other Ollie North.

People have to realize that the test of a policy or a program is not whether or not it is conducted in the open, but whether or not that the policy or program makes sense. What I hope is not lost in all the outcry from the public, the press, and yes, amazingly enough, the congress, for no more secret operations like the Iran/Contra program, is that, like it or not, the United States has to face the responsibilities of a superpower. And one of those responsibilities is the occasional necessity for secrecy.

Time Magazine concludes--and I agree--that if we are going to play the great power game, and ask others to risk their lives to help us win it, we had better accept the need for secrecy.

AN OPEN vs A CLOSED SOCIETY

Now, if you accept that premise, how do you square it against that thing called democracy, which, as I've said, tends to frown on anything that is not conducted out in the open? Of course, in an ideal world, I think we would agree, the affairs of state could be open for all to see. But with the likes of Khomeini, Ghadaffi and all those faceless terrorists running around the world, to say nothing of our good old adversaries in the Kremlin, we cannot enjoy the luxury of a completely open society.

Which does not, it seems to me, mean that we have to settle for a closed society, run by the government, where the people have no right to know what their government is up to, and

where the press is controlled by the government and can only print what the government says it can print. There are many examples of such societies around the globe and I doubt if anyone in this room would opt to live in any of them.

As anyone who has ever been there will attest, the Soviet Union is the classic example of a closed society. The people hear only what the party wants them to hear. In Moscow, if you don't know what you are looking for you won't find it--there are no signs on the buildings nor is there a telephone directory.

You can't criticize the government--there's no C-Span. There's also no fast food chains--the place is really the pits. It is a third-rate economy with a first-rate military.

We had a chance to talk to our ambassador to the Soviet Union, Arthur Hartman, when we were in Moscow, and he told us how difficult it is for our diplomats to operate there. The Soviet diplomats--spies in the US enjoy a tremendous advantage on our folks in Moscow. They have a far greater access to government officials, our scientific and technical organizations--think of the advantage the Soviets enjoy with the information we provide in the open--let alone the material that leaks out.

We are beginning to see signs of Gorbachev's attempts at openness, candor, and publicity--all summed up in the Russian word *glasnost*. Some early signs are promising--the release of Sakharov, more openness in the Soviet press--there was an unprecedented story last week in Pravda about the firing of a senior KGB officer who engineered the illegal arrest of a local investigative reporter. On the cultural front, the new line has created a literary pre renaissance. But it is far too early to determine if these represent real reforms or only empty rhetoric.

THE PRESS

So what do we do? How do we ensure that the government has the wherewithal to conduct certain operations in secret, that congress--or more accurately--that certain representatives in congress--are apprised of these secret operations, and that the public knows whatever it has a right to know about the operations of its government, through whatever mechanism, whether it be a free press, or through its elected officials or whatever?

And by the way, just as an aside with regards to the press, I'm sure a lot of you have the same feelings as I do about some of the press--the Sam Donaldsons and the Jack Andersons of this world. And during the last couple of months, we've had the press all over the place down at the committee and at times it can be quite a nuisance. But I read something the other day and I think it applies to the press, "If you want a watchdog to warn of intruders, you must put up with a certain amount of barking. If you muzzle him and leash him and teach him to be decorous, you will find he doesn't do the job that you got him for in the first place.

Some extraneous barking is the price you must pay for a service as a watchdog." I think that story also should be heeded by people in the executive branch when they think about congressional oversight.

And since I am part of that congressional oversight process, I thought I would focus on that as one way of dealing with the question I posed a minute ago, that is, "How do we ensure that the government has the wherewithal to conduct certain operations in secret, etc., etc., etc."

THE ABUSE OF POWER

As many of you remember, the intelligence oversight committees were established in the post-Watergate period as a reaction to Watergate and other excesses which made the public aware that there must be a constitutional guard, if you will, against the abuse of intelligence services by those in power. If the United States is to have an intelligence capability, the public must be assured that it remains an American intelligence capability, bound by the constitution and the law of the land.

Another concern which surfaced as a number of intelligence fiascos have come to light, has been that covert action programs carry with them a significant risk, particularly if there is little consensus on the foreign policy goals such programs are designed to serve. In order to make sure there is adequate accountability by responsible political authorities, formal oversight was seen as necessary. By the way, its sort of axiomatic that you accept that there is such a thing as a "responsible political authority." Without that assumption, we have no common ground for agreement.

Finally, and this is becoming more and more true all the time, the public has come to

recognize that we as a nation cannot afford to do everything. We have to make trade-offs between guns and butter. It's critical that a dollar's worth of investment produces a dollar's worth intelligence. As the budget officer that's my job.

THE VALUE OF OVERSIGHT

In sum, formal congressional oversight should help to keep our intelligence services healthy. It does this by providing an essential filter between the intelligence community and the public which it serves. One way that this filter operates is that it gives the intelligence community an opportunity to short-circuit actions which, for whatever reasons, may not have been fully thought out. Or they might be just plain stupid.

THE CASE OF NICARAGUA

A prime example of how this aspect of how oversight didn't work is the infamous CIA covert action operation in Nicaragua two or three years ago involving the mining of the harbors. Had the oversight committees had the opportunity to comment on this plan they perhaps could have pointed out how short-sighted and politically explosive the plan was, and thus could have saved CIA a tremendous amount of embarrassment and harm to its overall operation. There are still repercussions of that episode being felt by CIA today in its relationship with the Hill. You spend years building up credibility and you lose it overnight.

The same could be said, possibly, about the current situation involving the US policy towards Iran. Nobody in congress was consulted. And I know what you're thinking: If congress had been told about these programs the plans would have been leaked and the programs would never have gotten off the ground. Maybe, but I would argue that because you don't think the system works is no justification to abandon the system. We have laws and they must be followed. There are just too many success stories--which obviously nobody ever hears about--involving cooperation between the oversight committees and the intelligence service to hold that view, in my opinion.

Besides filtering out bad ideas, oversight can also provide a very useful service to intelligence agencies. There is no greater threat to intelligence than revealing how conclusions are revealed--the sources and methods. That is the *sine qua non* of our business. Now in the last

year or so there has been a great deal of consternation within the intelligence community and also, I can tell you, within the intelligence committees, concerning disclosures of certain intelligence information by government officials--including the president--to justify either a response to terrorism or to obtain the conviction of an accused spy. Some would question, and legitimately, I think, whether or not it's worth those results to give away sources and methods.

But there is an alternative that would allow us to it both ways. That is for the American people to be assured that the actions of the executive branch--an attack on Libya or a prosecution of a Pelton--are justified by the evidence--the intelligence--without having to reveal the sources and methods associated with that evidence. And that is for the oversight committees to know enough at the appropriate time to be able to say, in public "Mr. President, we have seen the proof and it justifies your response."

THE MATTER OF TRUST

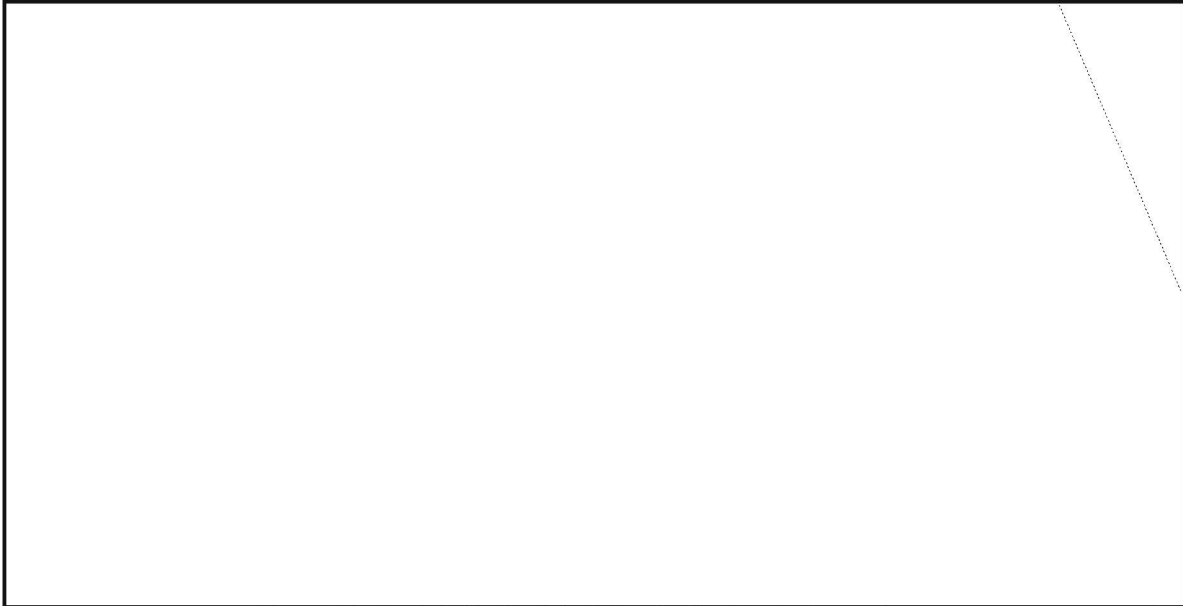
The key ingredient in that scenario is, of course, trust: Trust in the oversight process and trust in the actions and motives of the executive branch. Because at some point, let's face it, we simply must trust our leaders. But the must earn that trust. And trust and confidence in the oversight process is also critical and must also be earned.

Over the past ten years, this country has taken a major step toward building public trust by substantially strengthening the process of congressional oversight through the intelligence committees of the house and senate. Meeting the challenges of the coming decades will require continued strengthening and support for that process.

I don't pretend that these issues are simple or that there are easy solutions. Remember, we are dealing with a situation which goes to the core of the relationship between the legislative and executive branches of government. By definition, we are talking about bureaucracies and political bodies which make cooperation difficult at best. But our responsibilities to National Security--and to the values of an open and democratic society--demand nothing less.

~~TOP SECRET UMBRA~~

THE WAY WE WERE

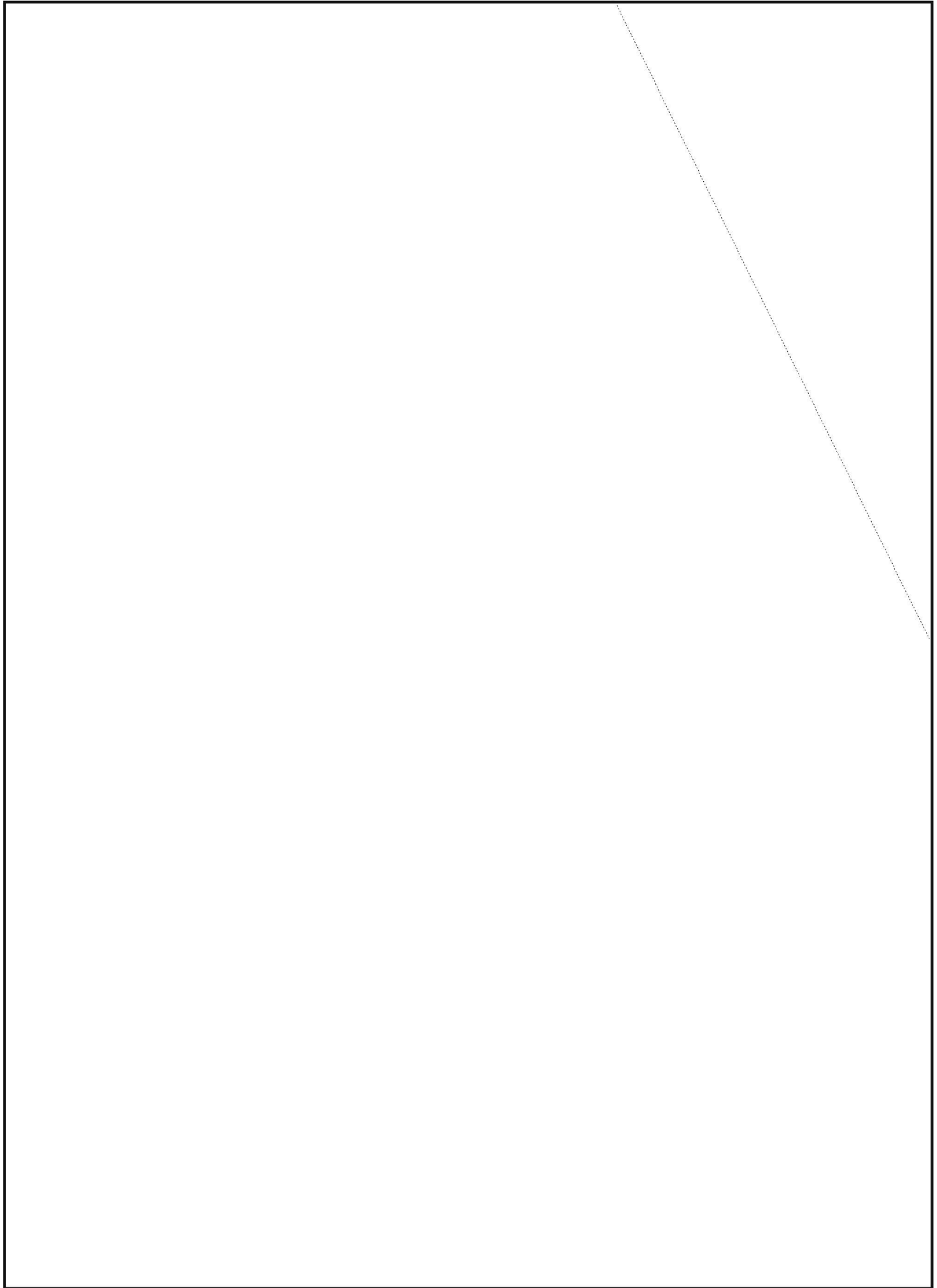


~~This article is classified TOP SECRET UMBRA in its entirety~~

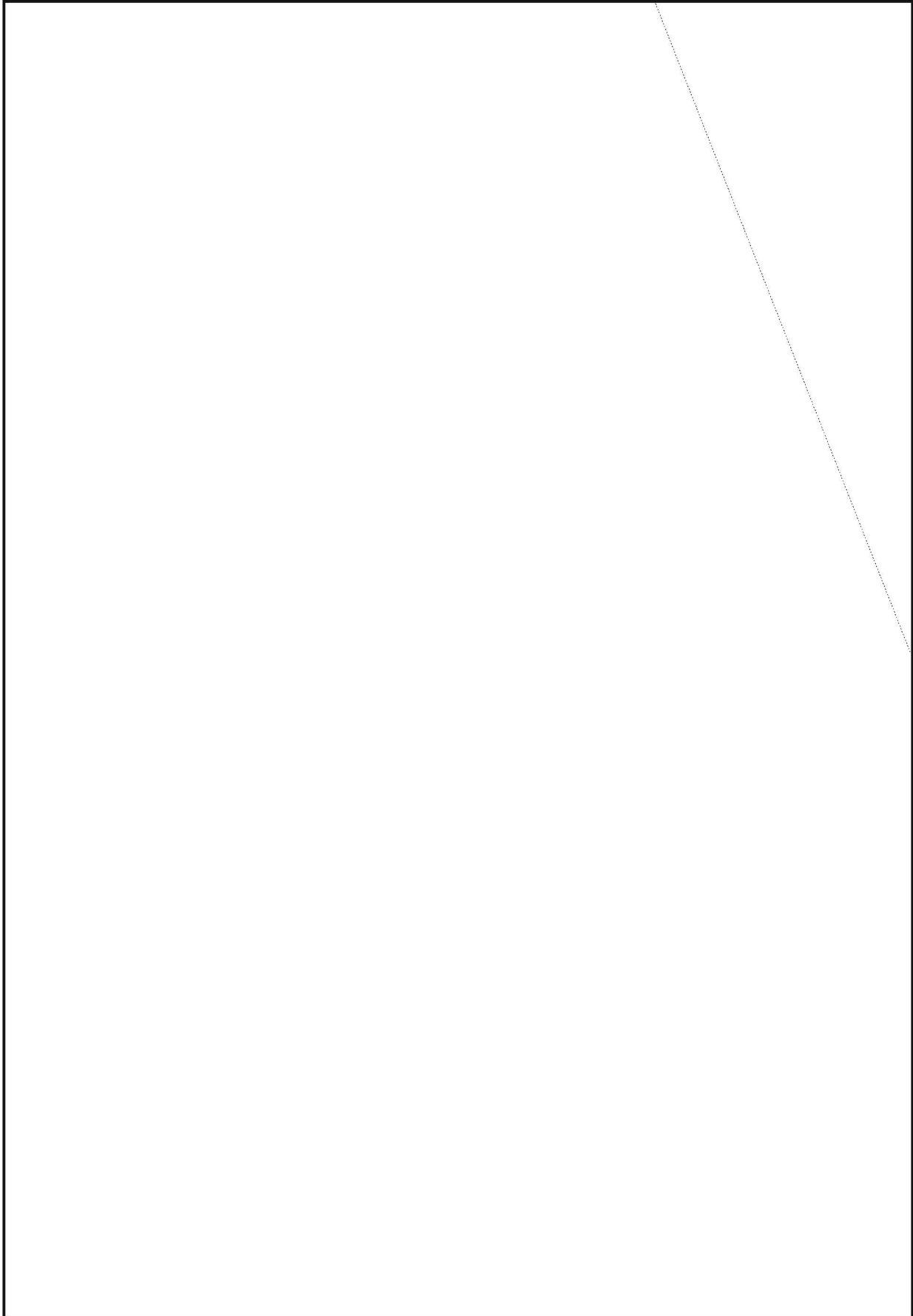


~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

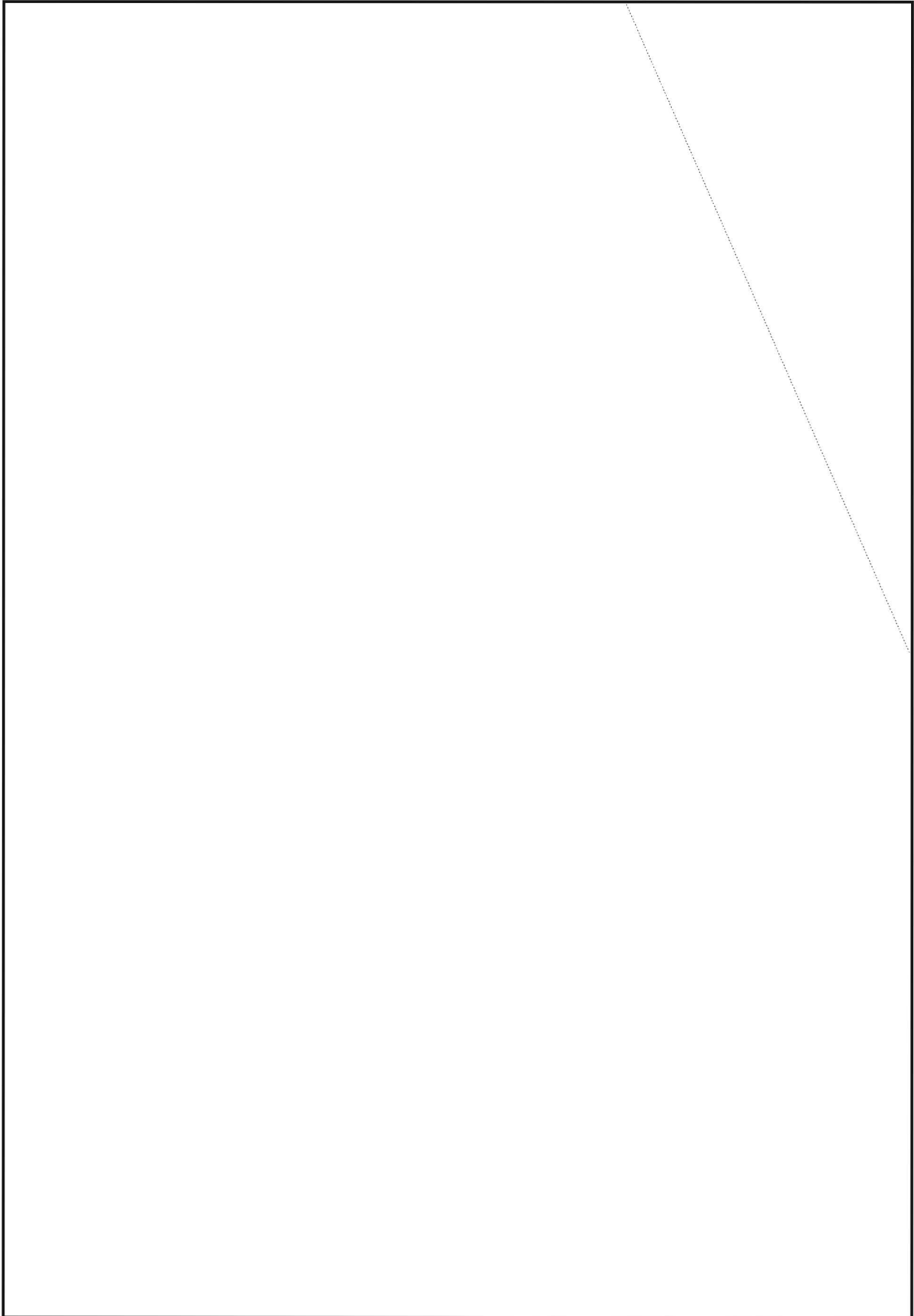


~~TOP SECRET UMBRA~~

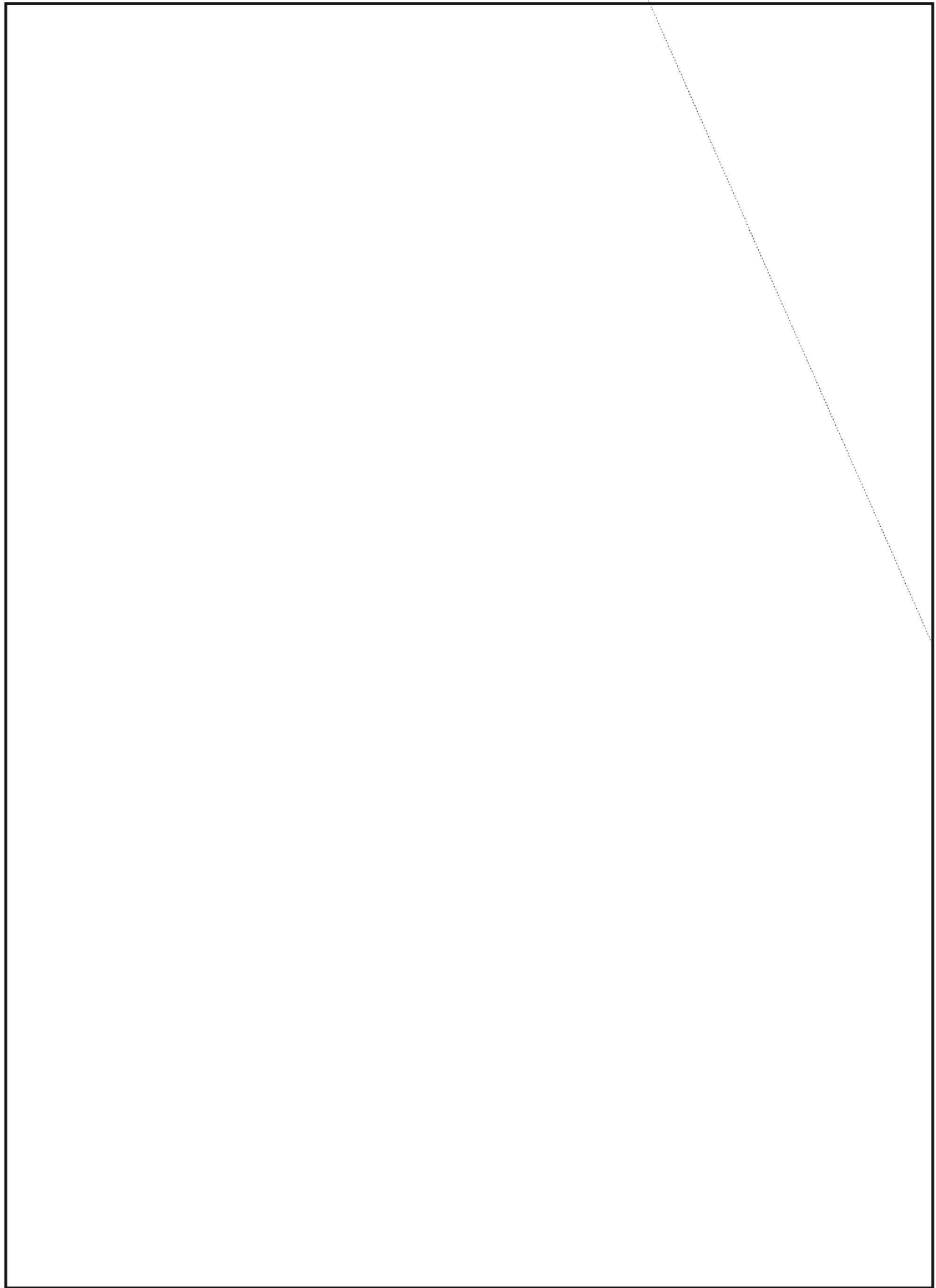


~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

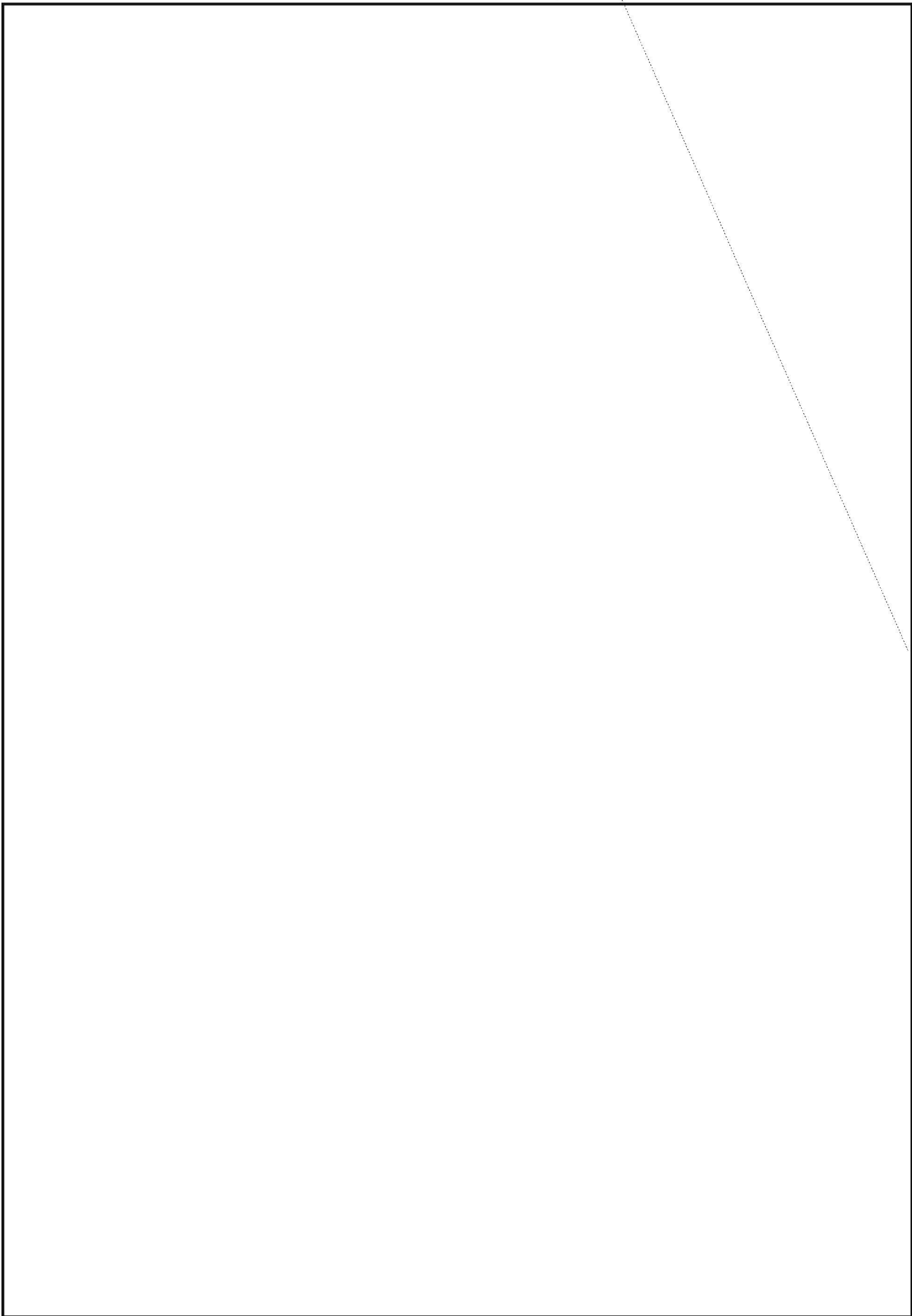


~~TOP SECRET UMBRA~~



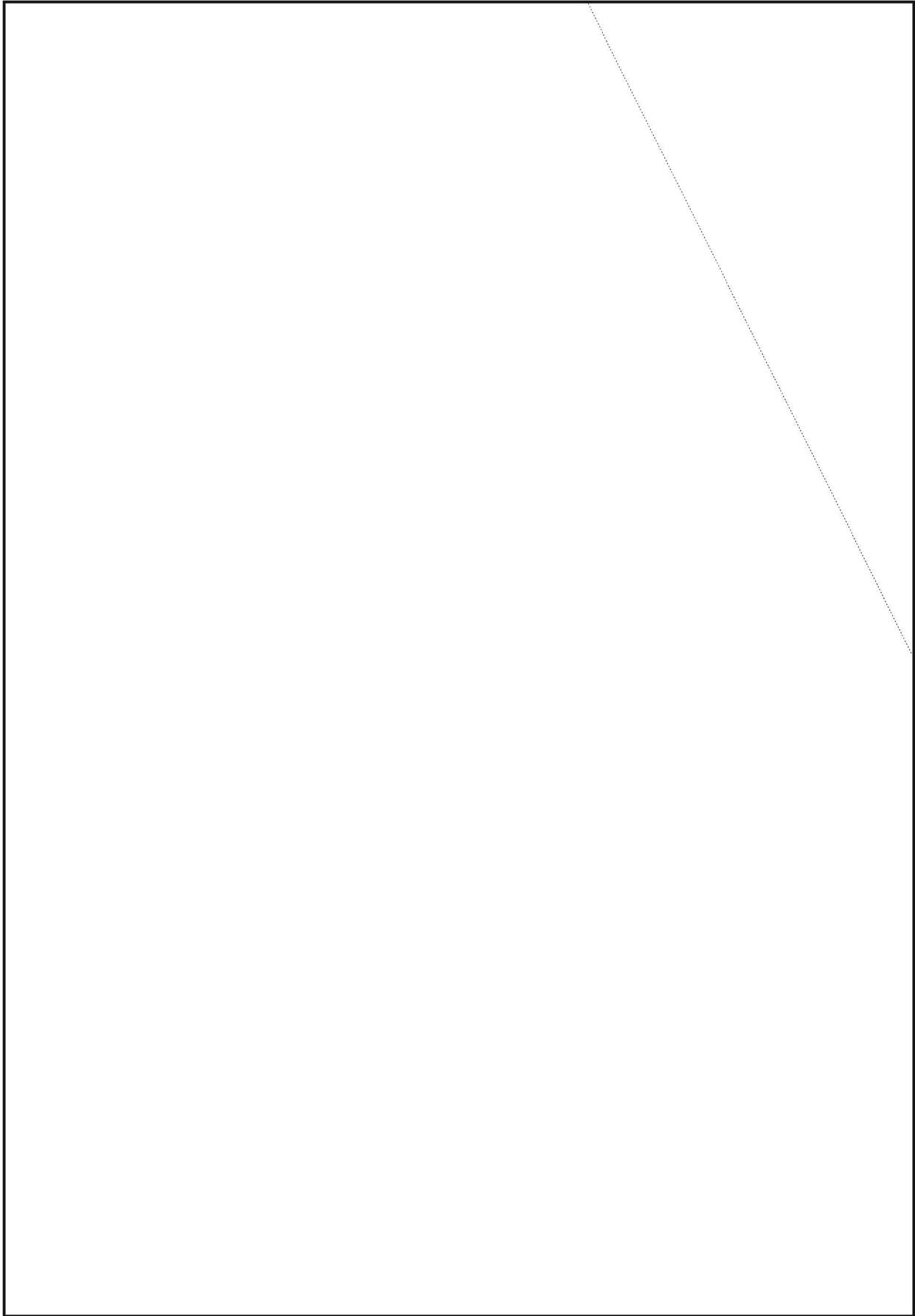
~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

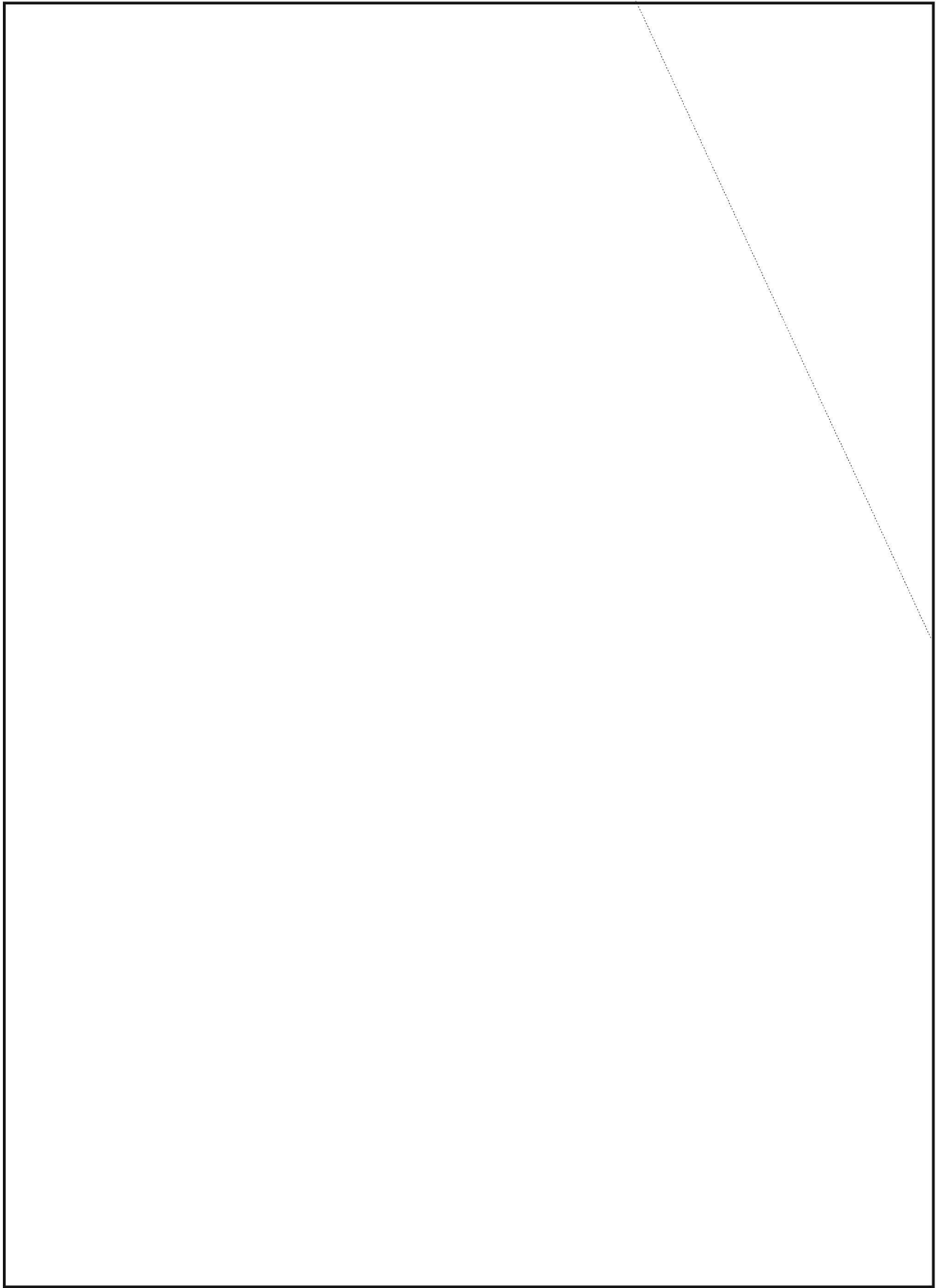


~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

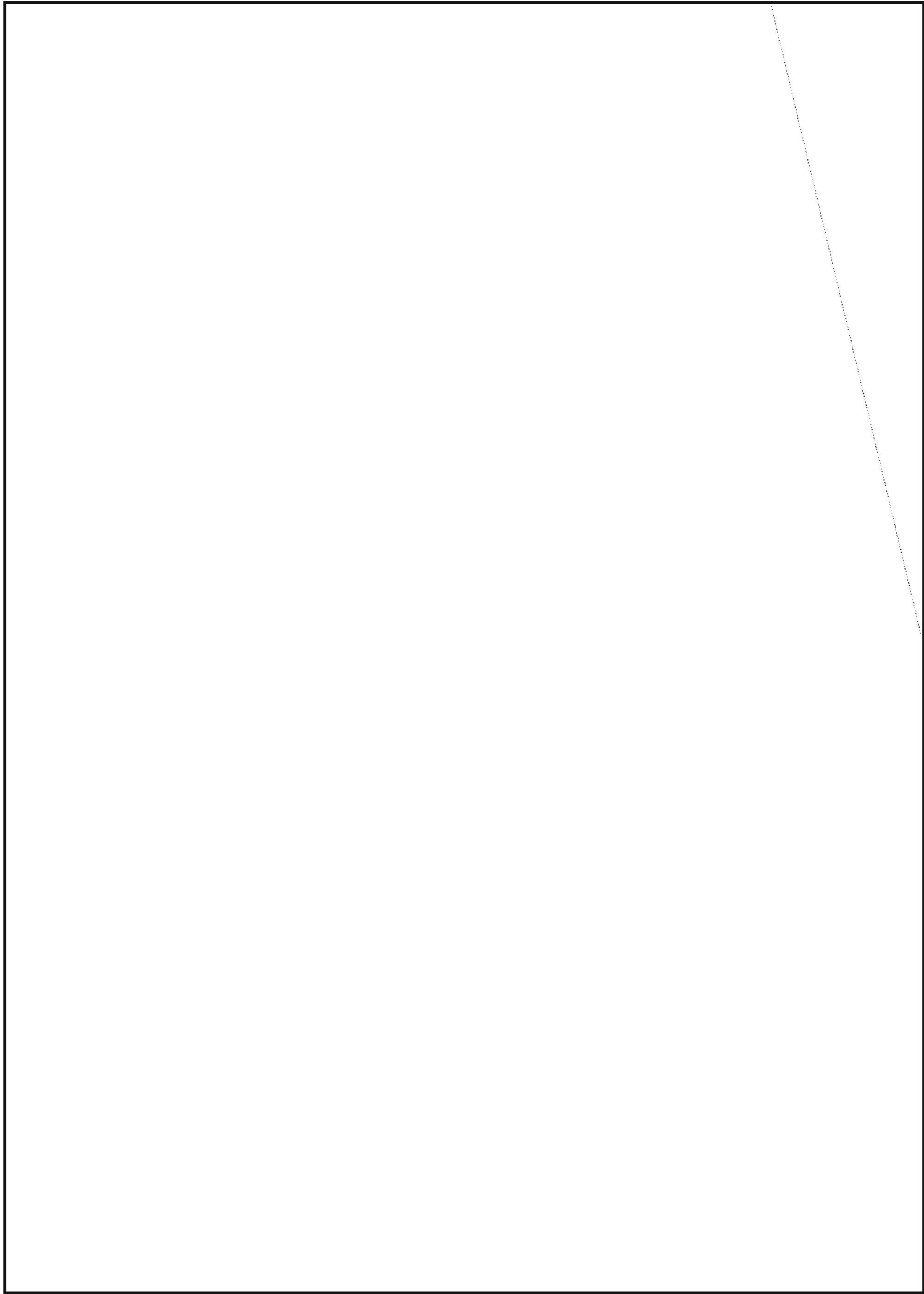


~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

~~CONFIDENTIAL~~

A View of L

Dale A Seaberg

The author was ADIL when he gave this talk at the third annual Federal Women's Program on 6 November 1985.

THIS ARTICLE IS CLASSIFIED
~~CONFIDENTIAL~~
IN ITS ENTIRETY

I am a business person and I run L like a business!

The type of business I run demands that I make the maximum use of all the people in the work force--both men and women. In terms of the female population in L, if I didn't make maximum use of their potential, I would be wasting 38% of my work force. In terms of population, L realized only a 2.5% population growth in FY84. The ratio between the overall female-male population has not changed more than 2% during the FY83-85 period.

In FY84 the male population decreased 2% with a corresponding increase to the female population. It's noteworthy to point out that in grades 7-11, which represent the largest segment of the L population (63% for men, 36% for women), the percentages of males and females correspond with the total female/male



population (62% for men, 37% for women).

Also, during the FY83-85 period, it is interesting to note that even though the female population in grades 13-15 decreased slightly (1%) from FY84, the female population in grades 7-12 increased by 43%. This high increase in population for women in grades 7-12 is significant because it suggests a tremendous amount of potential for women to attain the higher grades.

Other speakers during the Federal Women's Program have said the Agency must do better in promoting the women in our work force- especially to the more senior grades; and I agree with this. But, before you can promote women to senior grades, you have to make sure there is a sufficient number of women in the middle grades from which to draw. In this regard, L has an outstanding rate of promotion for women. To use a popular phrase, "What's the bottom line?" The bottom line is this: promotions in FY83,

This represents roughly a 50% ratio. This statistic compares to a 46%-53% male-female ratio in FY84, and evens out slightly in FY85, but with more women than men getting promoted.

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

~~CONFIDENTIAL~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~CONFIDENTIAL~~

Looking at the three years FY83 through FY85, there is one major point that should be made, and I'll ask a question before making it.

What are the percentages of male-female promotions against eligible male-female populations? The answer is:

PROMOTIONS			
	<u>Men</u>	<u>Women</u>	<u>Delta</u>
FY83	22%	38%	+15% for women
FY84	23%	37%	+14% for women
FY85	30%	50%	+20% for women

Again, this high rate of female promotions strongly suggests that there is a great deal more opportunity for advancement for women working in L. More so, I would guess, than most other Agency organizations. To quote Napoleon: "Ability is of little account without opportunity." What I try to do in L is to give all deserving employees an opportunity to advance.

Women supervisory positions are on the increase in L. So much in fact that since the figures for the briefing were put together, the number of female supervisors in L has increased by three. Indications are that with the rate of women promotions in L across the years we've looked at, the number of women supervisors will increase also.

In the area of training and from the standpoint of total female-male population [redacted]

[redacted] a slightly higher percentage of women than men receive training in L. In FY85, 73.7% of the male population received training against 77.5% of the female population.

As a business person, I want the best people to negotiate contracts, build buildings, manage supply systems, and defend logistics resources.

It doesn't make any difference to me if the person performing these functions is male or female. I push the women in L hard, maybe harder than the men. I do this because the women are as tough, fast thinking, and dedicated as the men. There is nothing that disappoints me more than a high potential woman who lacks confidence, drive, or commitment. There are not many women at higher grades in L, but looking at the percentage of promotions over the entire population, females have a higher ratio of promotions. This is because many of the types of jobs in L have not been traditionally women's areas in the past. However, we are breaking with tradition in this respect and are capitalizing on talent instead--and we will continue to do so!

The future for women in L is very bright. In recent years, more women in L are filling positions of contracting officers, engineers, illustrators, and programmers, as well as other positions that were male-dominated in the past. This is the result of a vigorous intern program in L, and a growing recognition that if we are going to be successful in the business we are in, we have to make the best use of all the people in the L work force. As far as I'm concerned, the L Organization offers a great deal of opportunity to anyone--female or male--with a commitment to do a good job.

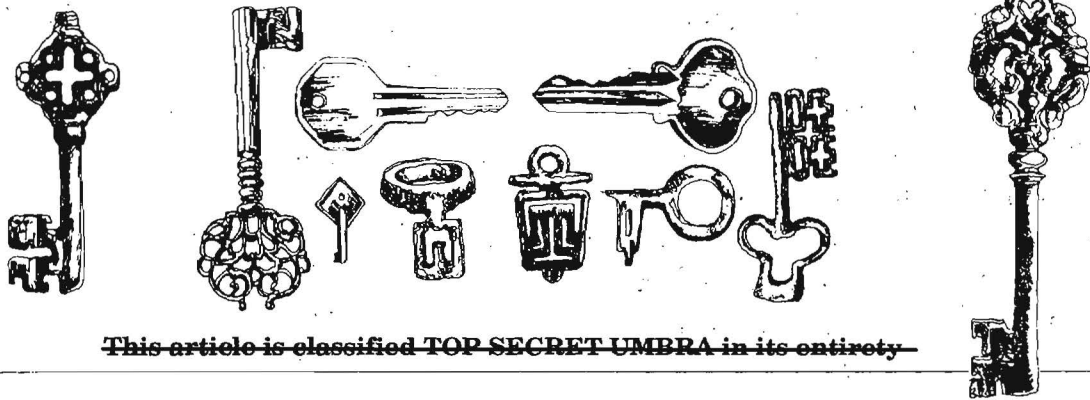
In conclusion, I'll paraphrase the old Chinese proverb, "Behind an able man there are always other able men". I would change that to: "Behind an able person there are always other able people." In the L organization, I am fortunate that there are many able people who carry out our important business.

~~CONFIDENTIAL~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

Keynote Address

Gerald R. Young, SUSLO



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

.....
 • This is a condensed version of the Keynote
 • Address to the 1990 session of CA-305,
 • Seminar on Contemporary Issues in
 • Cryptanalysis. At the time the author was
 • Deputy Director, NSA.
 •.....

I'm very pleased to have this opportunity to speak with you today! I think it's most appropriate that my first address of the new decade is to an audience of cryptomathematicians, cryptanalysts, and computer scientists because your work is at the very core of the work of our Agency.

Your past successes have aided immeasurably to further enhance the security of our nation and are central to the fine reputation our Agency has earned over the years. What's more, our future rests with you and your ability to meet the difficult challenges on the horizon. I challenge you to continue to be creative, bold and aggressive in finding solutions to the ever increasing number of cryptosystems being used in the world today and, in addition, providing the information security capability needed by the nation.

In a sense I believe conferences like this give us an opportunity to check up on ourselves and to see how we are doing and where we are going. Gatherings such as this symposium provide a real opportunity in bringing together the analysts from the SIGINT and INFOSEC communities to update

each other on significant successes, trends, and technological advances and, what's more, gatherings like this are essential catalysts to improving productivity and for making significant advances in your craft. I'm certain that each of you will come away from this seminar with some new and innovative approaches to apply to the problems you are working now or will be facing in the future.

As I reviewed the agenda for this seminar on Contemporary Issues in Cryptanalysis, I couldn't help but be impressed with the degree of sophistication in the technical work that is taking place in the Agency today. And it's important that we continue to make leading-edge, high-tech breakthroughs to keep pace with the rapidly changing world around us.

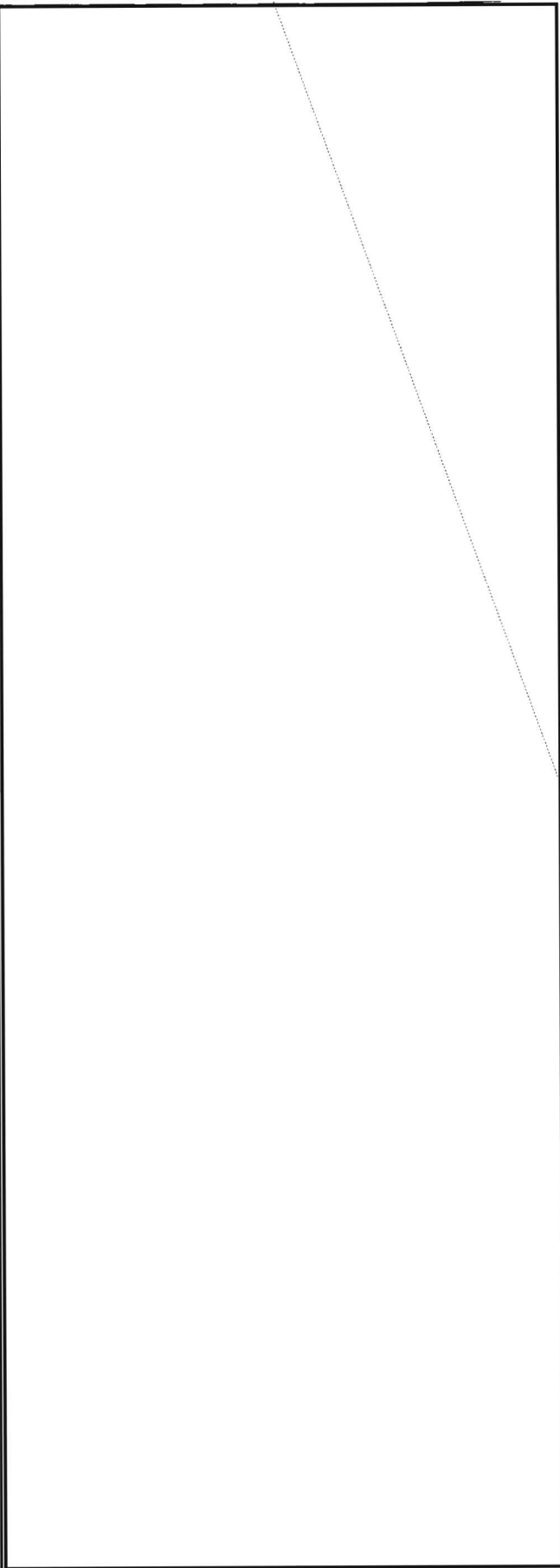
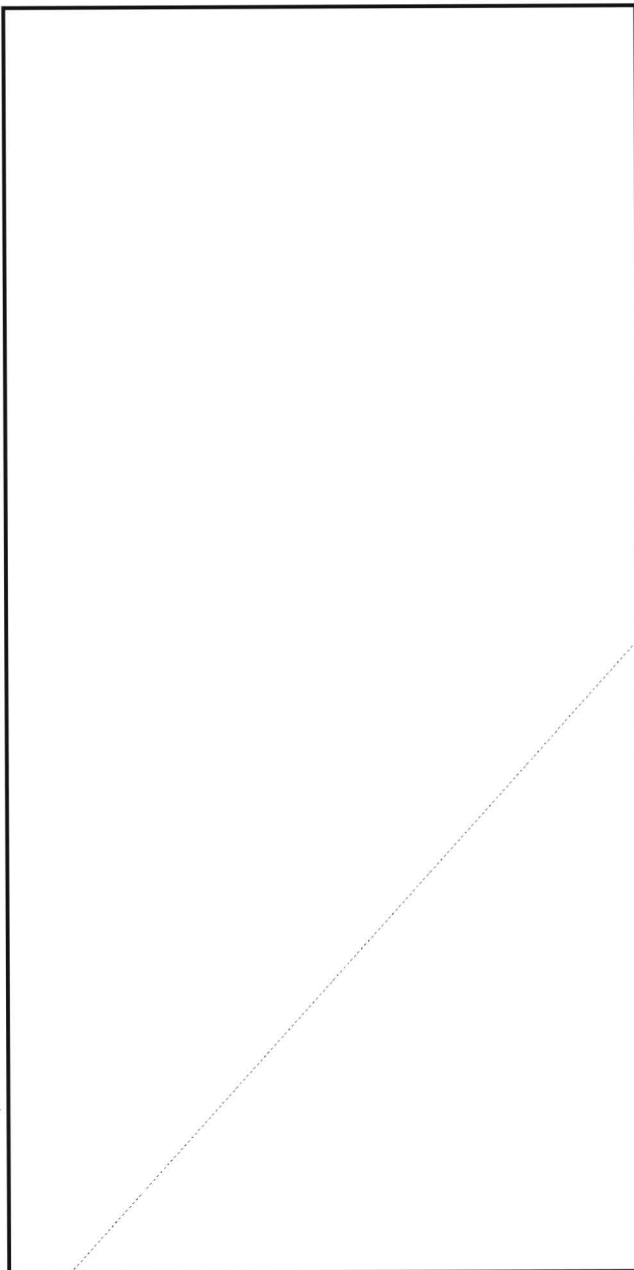
Today I'd like to share with you some of what I believe are the most significant trends and challenges we face, and along the way, I'll weave in some of the critical projects now underway that we must ensure are nurtured through the period of fiscal uncertainty facing us.

LOOKING AHEAD

Many so called "futurists" are still scratching their heads over the rapid, unforeseen changes that

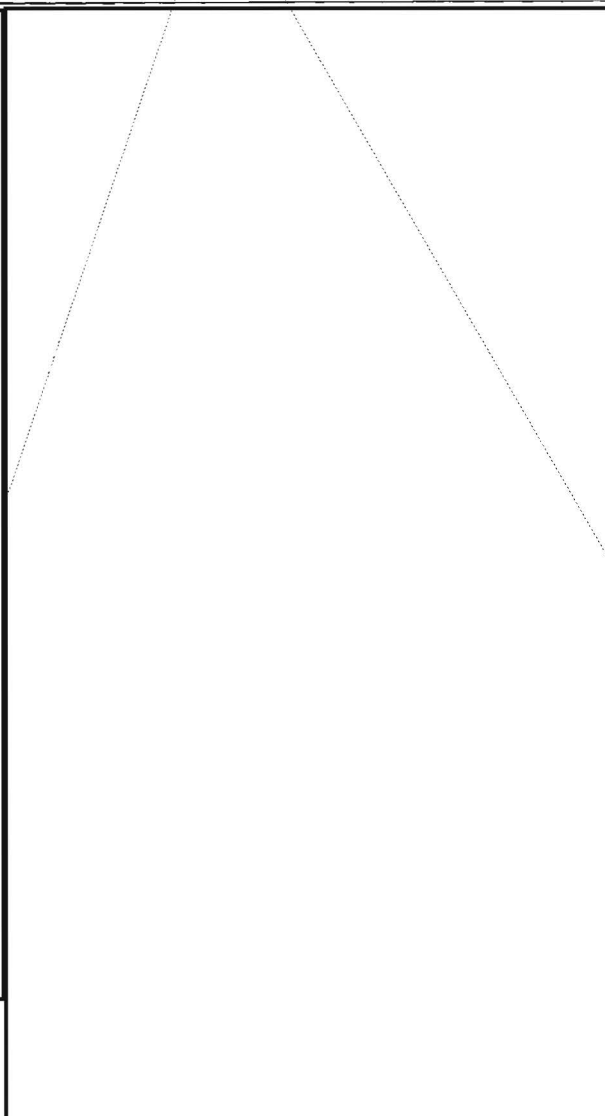
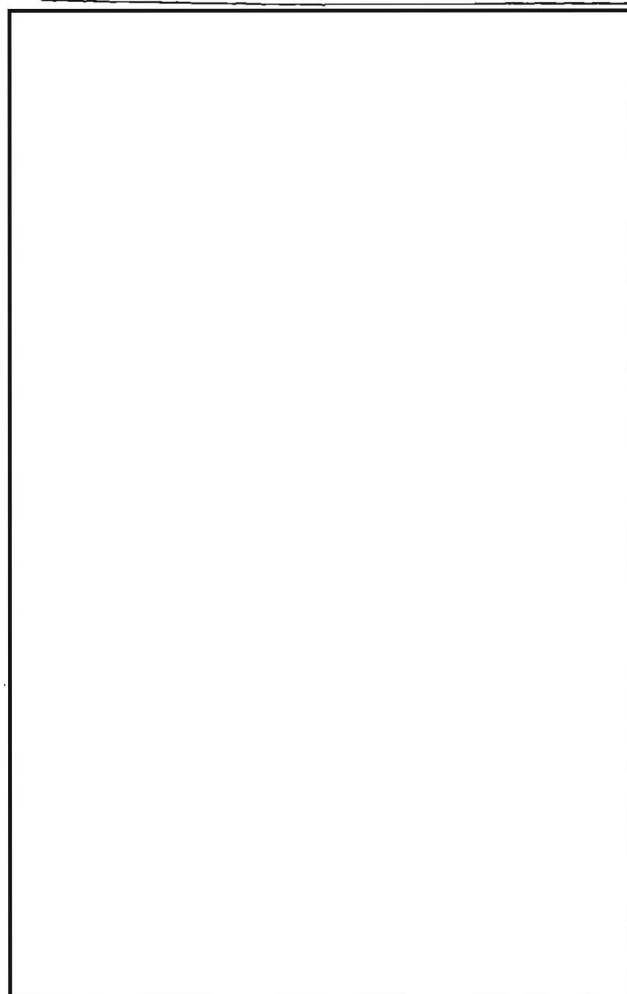
~~TOP SECRET UMBRA~~

have taken place in Eastern Europe. The true impact of these changes is still not clearly understood and it is yet uncertain how the dramatic changes in Europe will influence the intelligence requirements levied on us by our customers. With that in mind, let me dust off my own crystal ball. I'm reminded of the person who said the future is a bit like heaven—everyone exalts it, but no one wants to go there just yet! But the '90s are here so let me tell you what I sense are some of the major challenges facing the Agency.



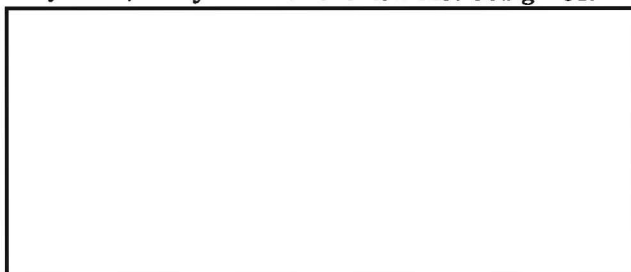
~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



Terrorism and Narcotics

Terrorist groups are also increasing the numbers and kinds of systems they are using. At any one point in time, we may work a large number of systems, many of which are now also using PCs.



INFOSEC

Advances in technology also are having a dramatic effect on our own INFOSEC world. During the week you'll be hearing about many of these technological breakthroughs and in addition, you will also hear about vulnerabilities found in some of our operational systems. However, just a word of caution—just as we have seen the proliferation of cryptosystems by our SIGINT targets, to include commercial and private sector targets, the United States is facing increasing demands to quickly design and evaluate increasing numbers of INFOSEC products.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

More and more US communications, both government and private sector, require protection by cryptography. As a result, we are faced with many more proposed INFOSEC products each year and we must balance our urge to accredit these systems with the credibility problems we'd face if we act too quickly and problems are later found in our "endorsed" systems. We can't afford to allow that to happen.

RESOURCES FOR THE FUTURE

Having stated some of our challenges, let me now spend the next few minutes addressing the current resources we have to meet these challenges. But before I do, let me relate a story which I believe is appropriate to the environment we are certain to face in the near future. It's a short story of a farmer who hired a hand and set him to chopping wood. In the middle of the morning the farmer went down to see how the hand was coming along. To his astonishment, he found the wood all chopped. The next day the farmer told the man to stack the wood in the shed. This involved a lot of work and the farmer figured the job would keep the man busy all day. But by noon, he had it all done.

On the third day the farmer thought he'd give the fellow a light job for a change and told him to sort out the potatoes in the bin. He told him to put the good ones in one pile, the doubtful in another and to throw out the rotten ones. An hour or so later he went back to see how the job was coming. He found the fellow passed out cold with virtually nothing done. After throwing water on the man's face and bringing him around, the farmer asked what had happened. "Hell, the man said, "The other work was easy. It's making all those decisions that's killing me!"

The prospect of hard choices is certainly facing us today.

People

As we make our choices, we must keep foremost in our minds that we have and will continue to need highly talented people, because it's the people who get the brilliant ideas that drive our efforts. It's folks like you that give our Agency its uniqueness, and although your contributions are well recognized by senior management.

I do not believe that the pool of people we need to get the cryptanalytic job done is going to grow substantially in the near future. We are entering some austere times. Therefore, we must seek imaginative strategies to gain further efficiencies and leverage to achieve our mission. We must place our people where they can make the greatest contributions. The CA Council is studying the manpower situation and has made recommendations to Senior Management which will be given very serious consideration as we formulate our plans and programs to deal with the multitude of challenges facing the Agency in the future.

The Cryptanalysis Intern and P1 Math Programs will bring new hires, but probably not a significant number of additional billets, to be used against the growing number of CA targets. For the near term, we expect the hiring for these programs to continue, with a modest number of new hires authorized for the CA Intern Program in FY 90 and a somewhat larger number for the P1 Math Program. The picture, however, is less clear for the individual cryptanalytic organizations. Most of the hiring in the Agency, at least in the foreseeable future, will be to replace attrition.

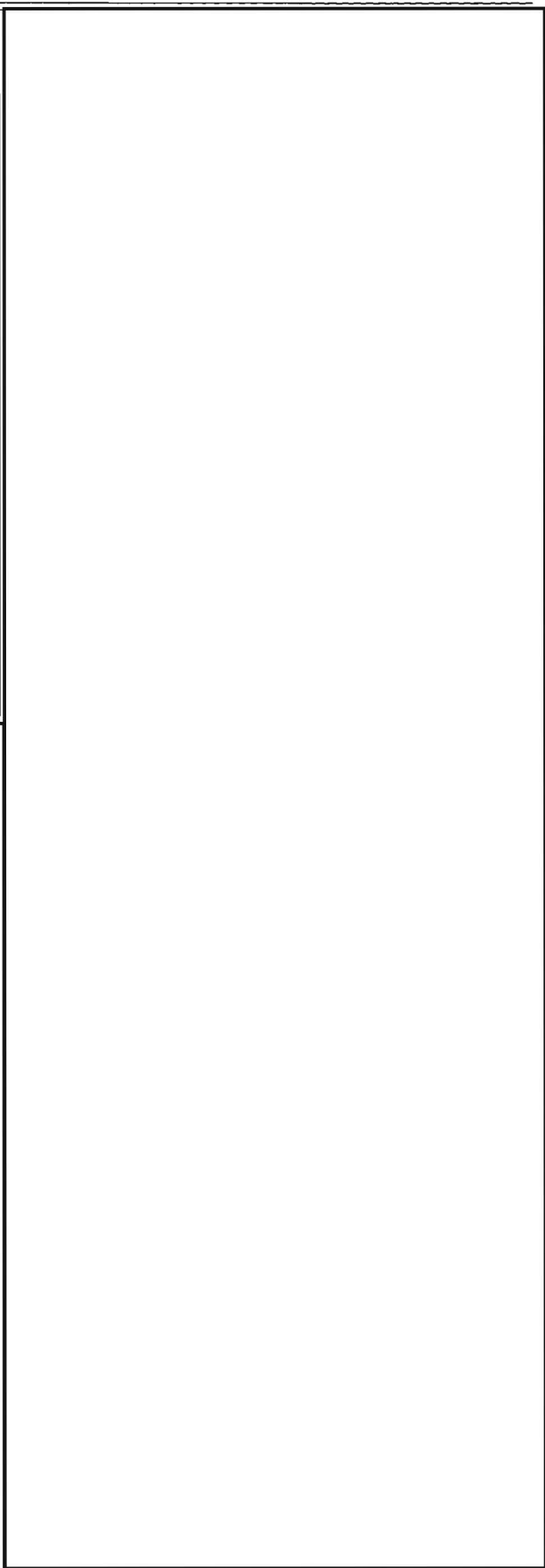
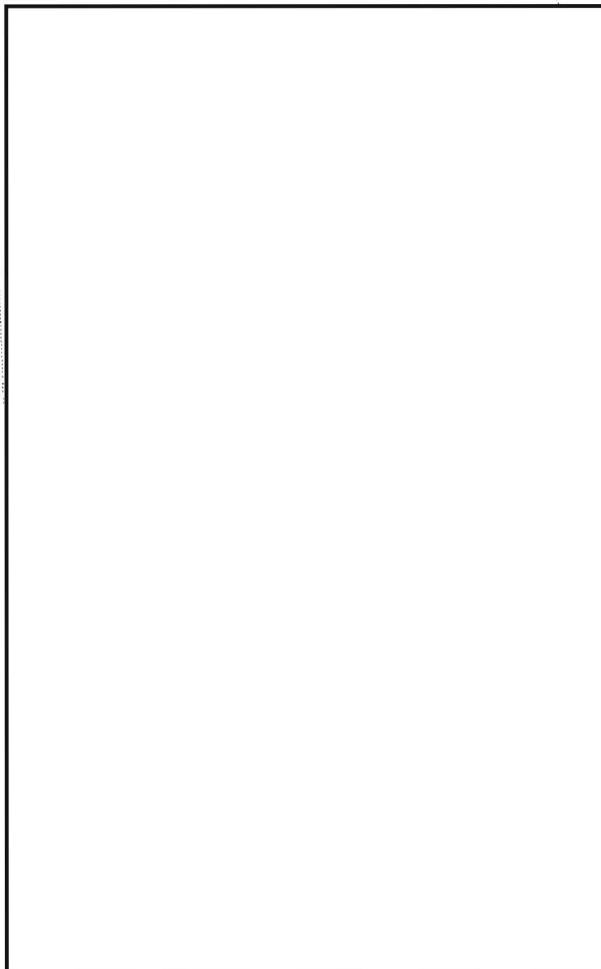
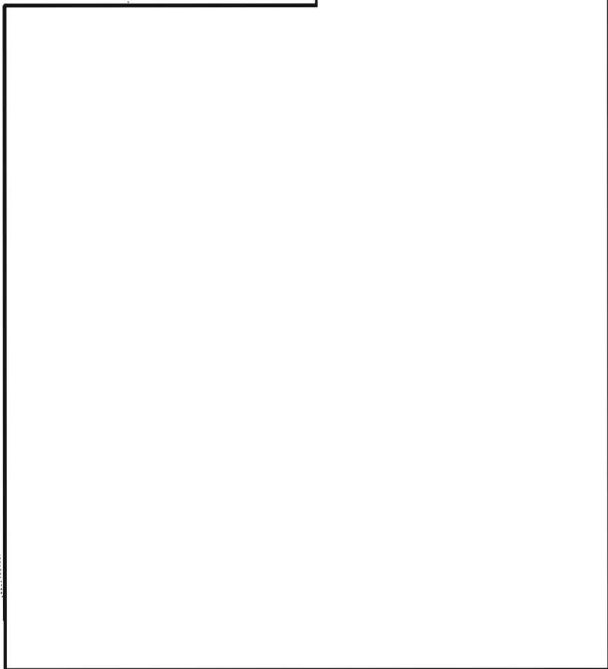
Supercomputers

Moving now to our equipment resources: As you know, our main sources of computing

~~TOP SECRET UMBRA~~

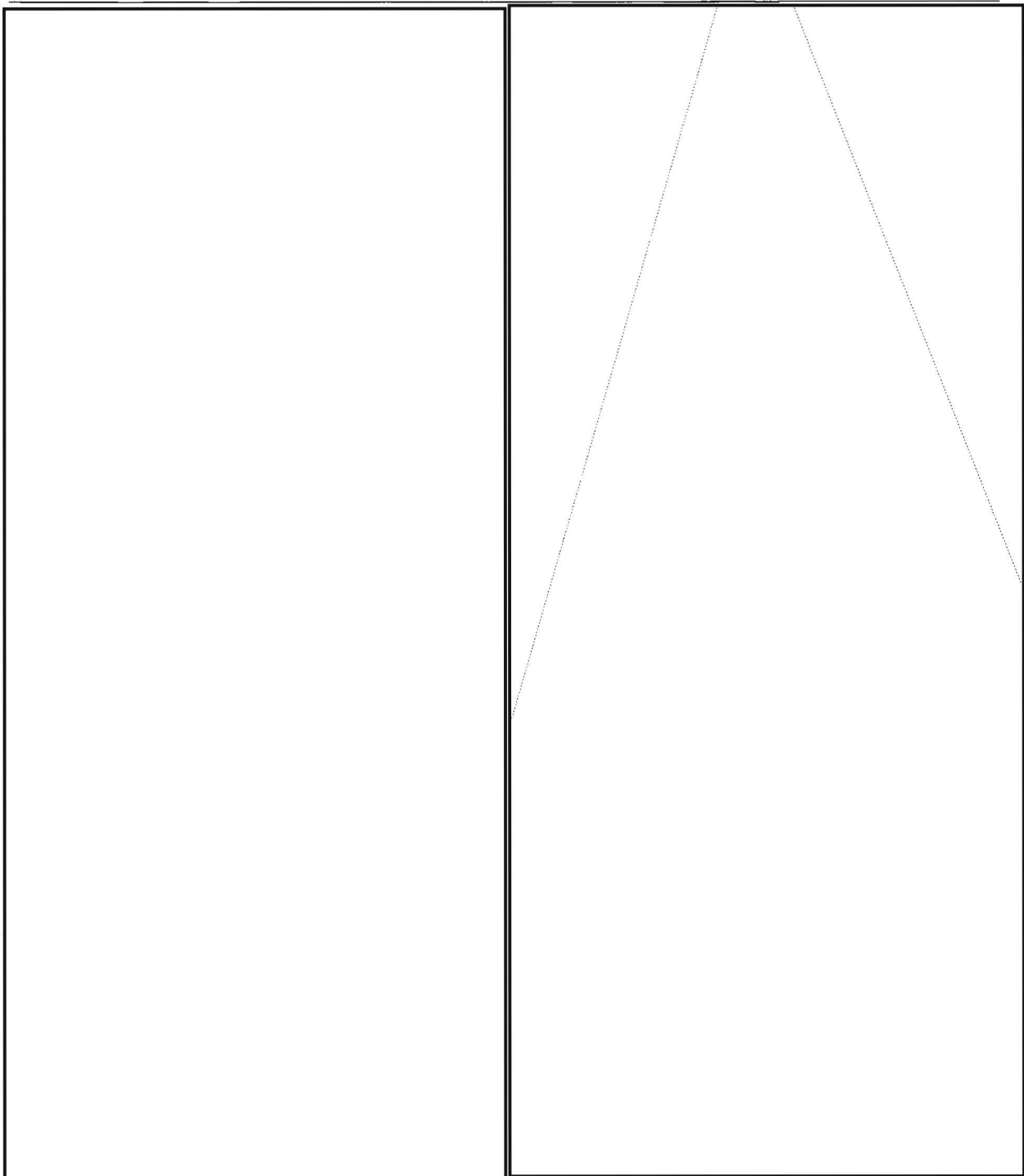
~~TOP SECRET UMBRA~~

equipment are supercomputers as well as the special-purpose devices we build when we can define a precise problem.



~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



New Cryptanalytic Techniques

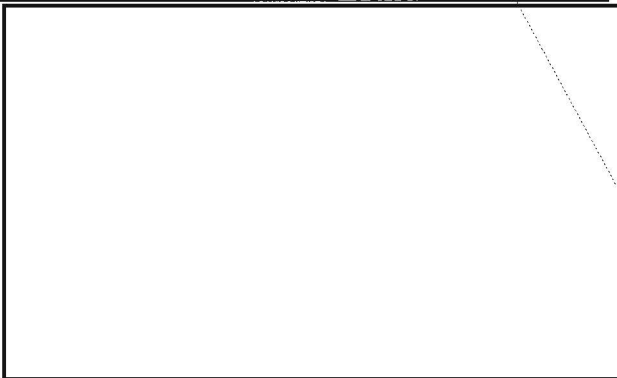
Another upward trend is in the development of new cryptanalytic techniques. From my work with the CA Council I believe we may be upon an age of new technique development. In particular, the conditional reestimation technique developed in conjunction with SRC holds great promise as a

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

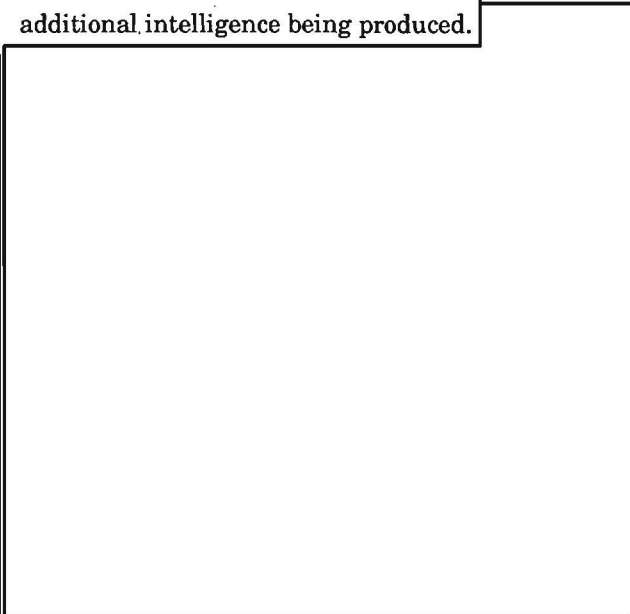
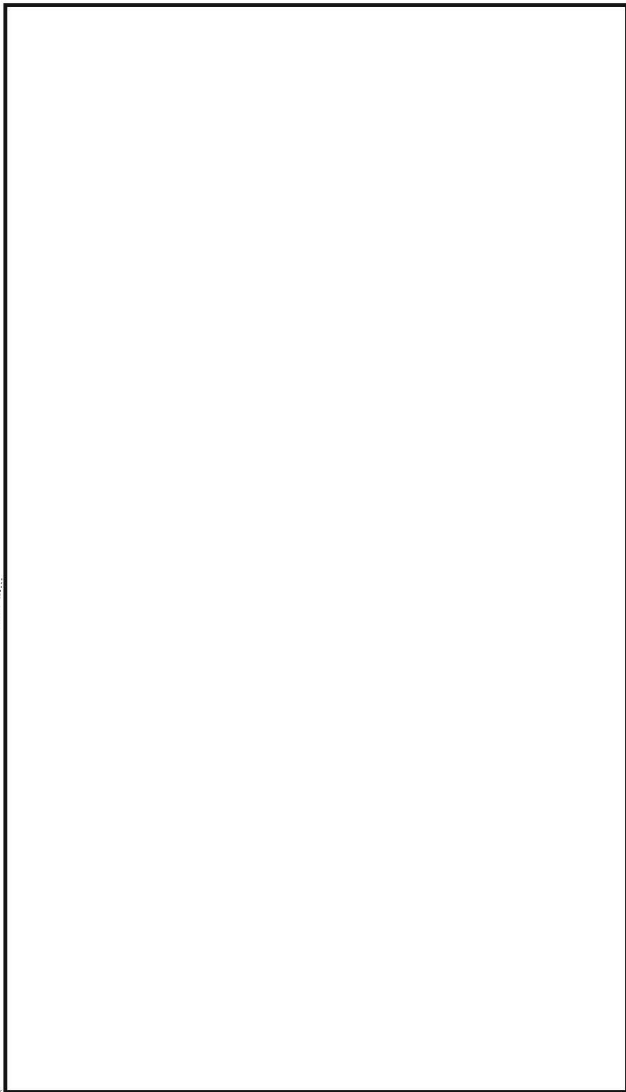
major new technique; it already has resulted in several successes and appears to have wide spread applications in both the machine and manual areas.

There are a number of other sessions this week on techniques including ones on cluster analysis, branching methods, discriminant analysis, the work on neural networks, the work on garbled linear equations, and others. I find the work on the "SPLASH" boards, where we are achieving Cray 1 and SPD power on the SUNs on some specific applications, especially impressive and the applicability of some of these advanced techniques to manual systems is also encouraging.



Management

I am optimistic that we will continue to have successes against our targets and in our own INFOSEC efforts. The reorganization in 1987/88 of the G Manual effort will continue to pay off with additional intelligence being produced.



In closing, let me say again that we face many formidable challenges, but I am confident that we are up to those challenges. Given your continued dedication to the problems, I'm optimistic that we will continue to achieve significant cryptanalytic successes against our SIGINT targets and in the area of Information Security.

Thank you again for allowing me to speak with you this morning and I wish you a useful, productive week.

□

~~TOP SECRET UMBRA~~

From the Past

Categories of NSA Specialties

PERS Planning Group

S/SST

8 Jan 54

(Mr. Friedman)

1. In reference to your DF, dated 22 December 1953, subject: "Categories of NSA Specialties," it appears that the committee concerned made an effort to establish general categories of specialties along functional lines. This is considered a good initial step.

2. After studying the proposed list, some of the specific observations made include the following:

(a) The functions of P/P, LOG, PERS, and TNG are completely omitted. In order to execute the Agency's War and Disaster Plans, skilled personnel will be needed to fulfill some the functions of each of these.

(b) Under the group title, Cryptographic Equipment and Material, the listed functional specialties of Research, Design, and Production omit the functions of Procurement, Maintenance, Distribution, and Accounting. Further, this group seems to be overlapped, if not duplicated, by a group titled "Crypto-Material."

(c) Under the group title, T/A, are listed several functions. However, the entire incoming sorting and distribution functions are omitted. Further, it would seem reasonable to include Radio Telephone and a specific reference to the [redacted] functions.

(d) The listings under Crypto-Linguists seem to omit the need for linguists who are no necessarily cryptanalysts.

(e) The group title [redacted] is itself a misnomer. In regard to the [redacted] functions listed, it would seem appropriate to include the functions of Procurement, Operation and Maintenance.

(f) Under the group title, Mathematics, it might be desirable to include specific references to those personnel currently familiar with applied key studies, theoretical research, and long-term machine programming.

(g) Under the Weather function, it might be well to include specific references to weather [redacted] etc.

(h) The functions listed under Management are not clear.

(i) The functions listed under Communication omit operations.

3. The following observations are made:

(a) The suggested list of NSA specialties cover some broad functions, and a few specific functions.

(b) Some broad functions necessary to execute the Emergency War and Disaster Plans and to sustain the Agency under emergency conditions are omitted.

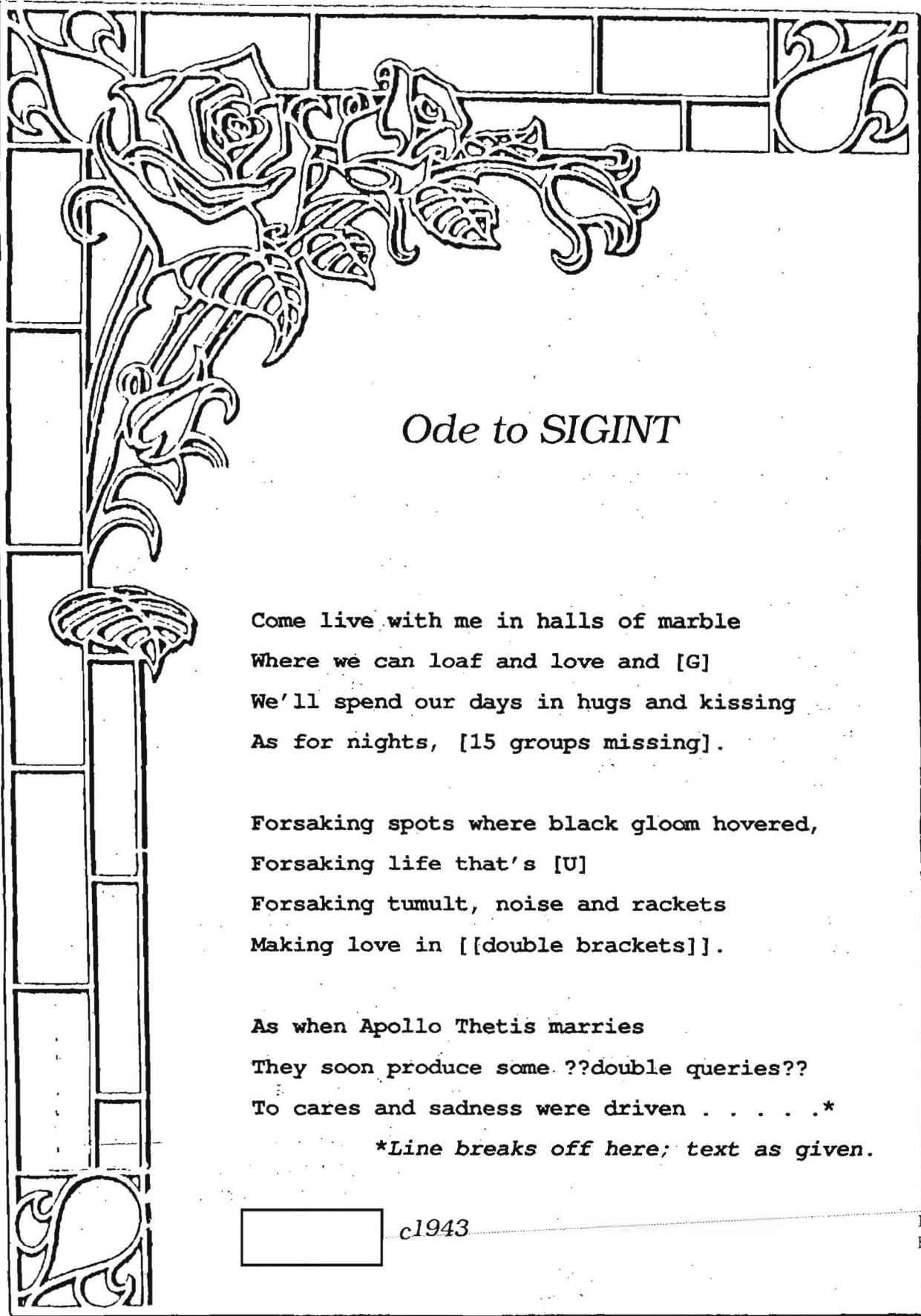
4. In the light of the foregoing, it is suggested that:

(a) The next group who meet to discuss this problem include personnel who are familiar with the overall NSA mission and the Agency's War and Disaster Plans.

(b) The suggested list be expanded into a more complete list of critical NSA functions and that it be made more specific so that ultimately the names of personnel can be inserted into the list down to the level required for the successful execution of the Agency's War and Disaster Plans.

WILLIAM F. FRIEDMAN
Special Assistant

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



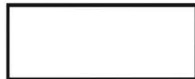
Ode to SIGINT

Come live with me in halls of marble
 Where we can loaf and love and [G]
 We'll spend our days in hugs and kissing
 As for nights, [15 groups missing].

Forsaking spots where black gloom hovered,
 Forsaking life that's [U]
 Forsaking tumult, noise and rackets
 Making love in [[double brackets]].

As when Apollo Thetis marries
 They soon produce some ??double queries??
 To cares and sadness were driven*

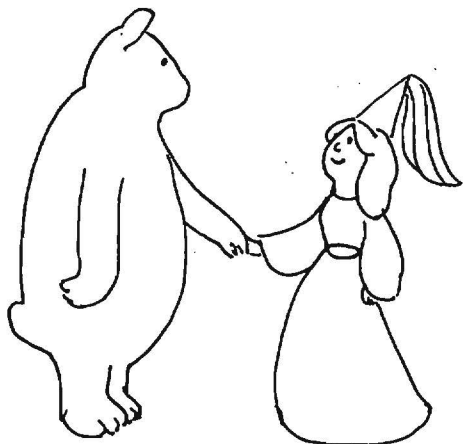
**Line breaks off here; text as given.*



c1943

E.L. 86-36
 FO 1.4.(c)

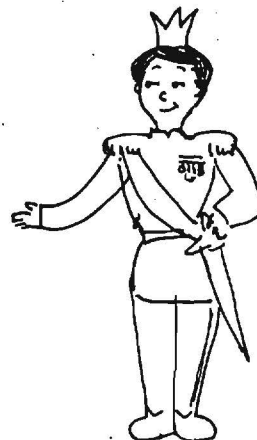
A Modern Fairy Tale



Once upon a time a fair damsel lived in the Kingdom of the Brown Bear.

The King of Centralia offered her a position of power in his kingdom. There she did many wondrous things and became well known in the scattered kingdoms of the Kingdom.

For example, the King of the Kingdom of All Other Kingdoms appreciated her efforts on behalf of his subjects. He was content that she should remain in her position in the Kingdom of Centralia and help all the subjects of the realm.



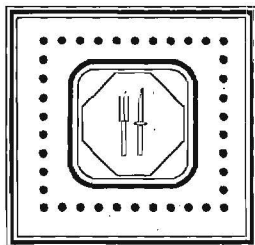
On the other hand, the King of the Kingdom of the East, also known as the Dragon of the East, or, less affectionately, as the Beast from the East,

decided to lure her into his kingdom to do service only unto his subjects.

He offered her three inducements to make this change.



The first was a dingy cave for an office in contrast to the palatial quarters at Centralia.



The second was an opportunity to spend two feeding times a week with the King and Queen of the Kingdom of the Brown Bear, the King and Queen of the Kingdom of All Other Kingdoms, the King of the Kingdom of Centralia, and the Wizard of Things Manual.

Their mission was to draw up a unifying plan for all the kingdoms, and they became known as cohortus octo, an expression of scorn throughout the realm as 21 months of this brought them no closer to success even to this day.

The third inducement was the most unkindest cut of all. She would rule at the side of the Beast from the East instead of in a position of great power with the kindly King of Centralia.

Who would take such an offer? The King of Centralia consulted with the Wizard of Things Manual and they concluded that the Dragon of the East had cast a spell on the hapless victim!



And now to the sad conclusion of this modern fairy tale: for there was no way to break the spell except to take an early out from the Kingdom.

So Godspeed, Fair Barbara.



This Way Out

An oration on the occasion of the retirement of [redacted] September 1991, composed and delivered by [redacted]

P.L. 86-36

CRYPTOLOG

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 @ bar1c05
 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

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. XVIII, No. 3 3rd Issue 1991

PUBLISHER [Redacted]

BOARD OF EDITORS

- EDITOR [Redacted] (963-1103)
- Computer Systems [Redacted] (963-1103)
- Cryptanalysis [Redacted] (963-5238)
- Cryptolinguistics [Redacted] (963-4382)
- Information Resources [Redacted] (963-3258)
- Information Science [Redacted] (963-3456)
- Information Security [Redacted] (972-2351)
- Intelligence Reporting [Redacted] (963-5068)
- Language [Redacted] (963-3057)
- Linguistics [Redacted] (963-4814)
- Mathematics [Redacted] (963-5566)
- Puzzles [Redacted] (963-1601)
- Research and Engineering [Redacted] (968-7315)
- Science and Technology [Redacted] (963-4958)
- Special Research Vera R. Filby (968-5043)
- Traffic Analysis [Redacted] (963-3369)
- Classification Officer [Redacted] (963-5463)
- Bardolph Support [Redacted] (963-3369)
- Clover Support [Redacted] (963-1103)
- Macintosh Support [Redacted] (968-7315)
- Illustrators [Redacted] (963-3360)
- [Redacted] (963-4382)

P.L. 86-36

To submit articles and letters, please see previous page

For New Subscription or Change of Address or Name

MAIL name and old and new organizations and building to:

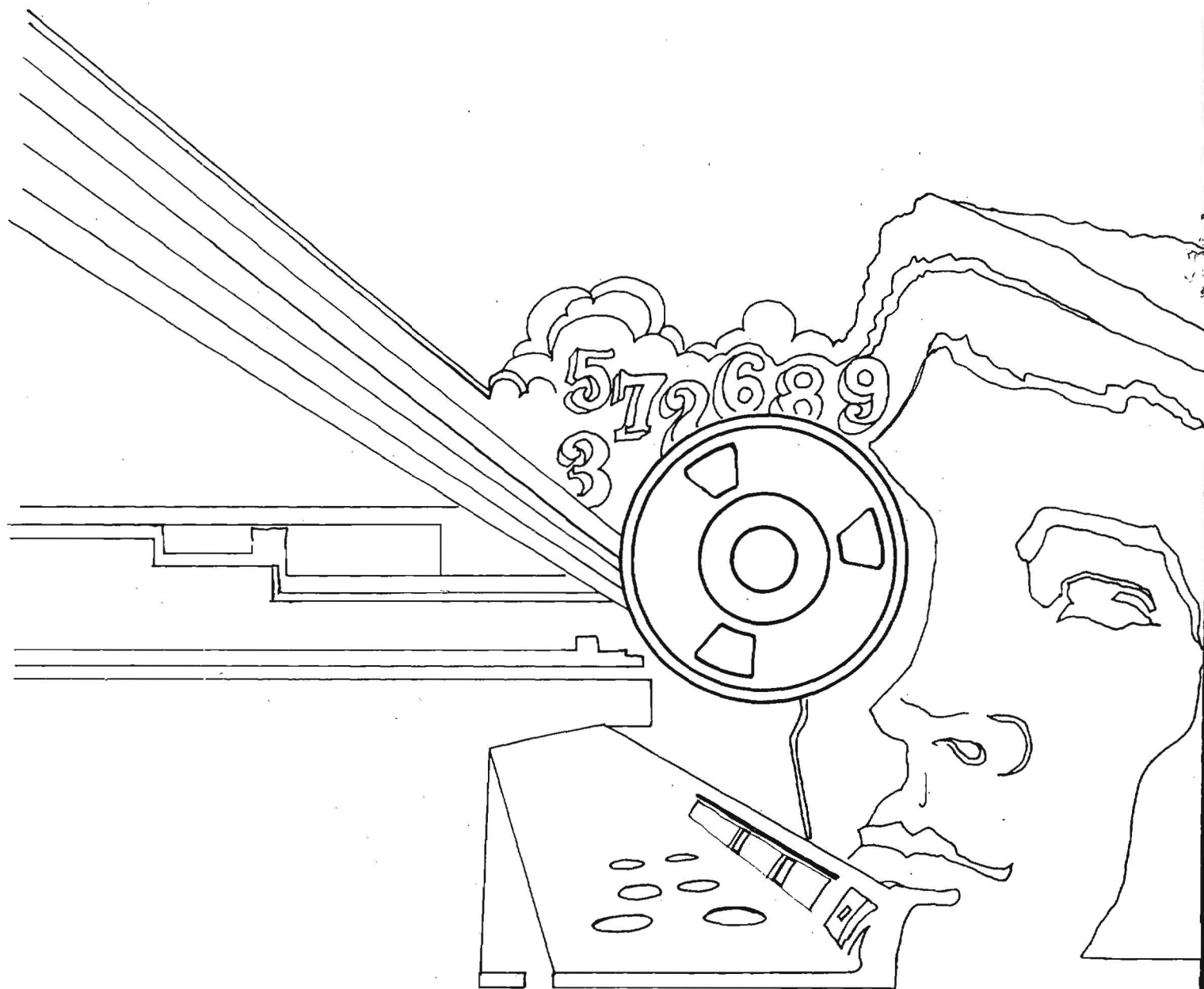
Distribution, CRYPTOLOG, P1, NORTH
 or
 via PLATFORM: cryptlg@bar1c05
 via CLOVER: cryptlg@bloomfield

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

Contents of CRYPTOLOG may not be reproduced or disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

All opinions expressed in CRYPTOLOG are those of the authors. They do not represent the official views of the National Security Agency/Central Security Service.

~~TOP SECRET~~



~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~NOT RELEASABLE TO CONTRACTORS~~