NATIONAL SECURITY AGENCY
CRYPTOLOG

CRYPTOLOG

Board of Advisors

To submit articles and letters, please see last page

Table of Contents

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

P.L. 86-36

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

A Note from the Chairman:

THE CRYPTOLOG IN A TIME OF CHANGE

The end of the Cold War, the redefinition of vital U.S. interests, increasing fiscal cutbacks, downsizing of the technical workforce, and the proliferation of complex technologies provide the impetus for revitalizing the CRYPTOLOG.

First and foremost the CRYPTOLOG will remain a forum of the informal exchange of information by the analytical-technical workforce and will serve to enhance the knowledge base of technical skills within the SIGINT community.

But in these incredibly rapidly changing times it should also address the purposes Dave Gaddy described in a 1989 CRYPTOLOG article entitled "Where Are Our Textbooks?": "professional literature is...a means through which the profession is defined and...grows and evolves over time. It affords the opportunity to assert and to challenge, to advance ideas and...expose outdated thinking and procedures. It can also supply a more systemized institutional memory, such as that called for by NCS Commandant Whitney Reed in a 1988 memorandum to Agency seniors: 'we are heavily dependent on individual knowledge, recollections of lessons learned (and not learned), and acquired wisdom on the part of our seniors to guide the education of the next generation of Agency leadership.'"

In that spirit, and in an attempt to make the Cryptolog a more relevant and useful publication, I and the new board of advisors invite you to contribute articles, letters and reviews to the Cryptolog which:

- address current and future issues and directions in your field and in the technical aspects of the target and the SIGINT process

- promote understanding and appreciation of the worldwide advances in technology and the changes in the SIGINT process required to respond to them, i.e. technical matrixing.

- describes strengths and, more important, weaknesses in how we have gone or go about our business, e.g., lessons learned, histories etc.

- enlighten the workforce on breakthrough technical advances which could significantly affect all aspects of SIGINT

- disseminate information on professional seminars attended

- encourage discussion and even debate among experts on any controversial subject affecting technical health.

Finally, this journal can serve as a voice of the technical track.

P.L. 86-36

Chairman, CRYPTOLOG Board of Advisors
Ext. 963-7712s

Intelligence & Combat:

P.L. 86-36

Some Lessons From DESERT STORM

by [ ] P054

(FOUO) We in the SIGINT business have long recognized that direct access to the principal player in a given scenario is far more likely to yield accurate and reliable assessments than would be available if we're reduced to listening to what other interested, but perhaps not all that well-informed, sources have to say about that same situation. It was with great anticipation, therefore, that an overflow crowd turned out on 15 April to hear an address in the Friedman Auditorium by United States Air Force Colonel Chris Christon, then the Director of Intelligence, USAF SPACE COMMAND and formerly the Air Intelligence Officer for Lt. Gen. Charles Horner, Commander, Coalition Air Forces, Gulf Theater, during Operation DESERT STORM. Col. Christon—by any definition a principal player during the allied operation to drive the invading Iraqi forces from Kuwait—shared with the assembly his experiences in Saudi Arabia, emphasizing the intelligence successes but, more important, driving home some lessons learned about how to use intelligence to support the kind of warfare that our national security strategy and our force posture will dictate in the future.

How good was intelligence support to DESERT STORM...

> *"In combat, everything starts and ends with intelligence."* —Lt. Gen. Charles Horner

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

1

CRYPTOLOG
July   1994
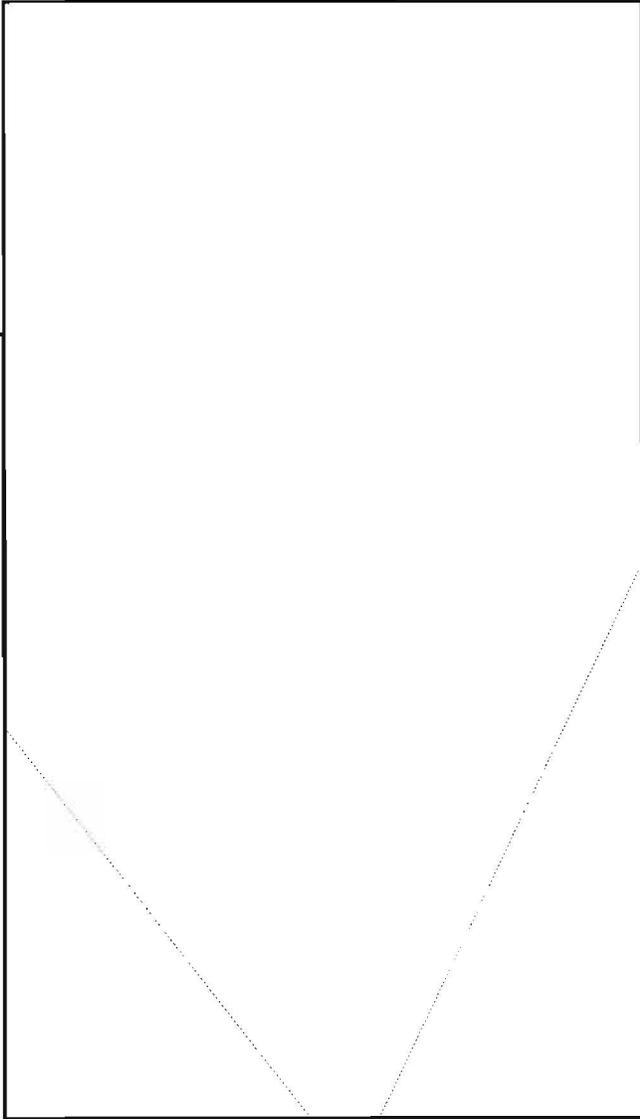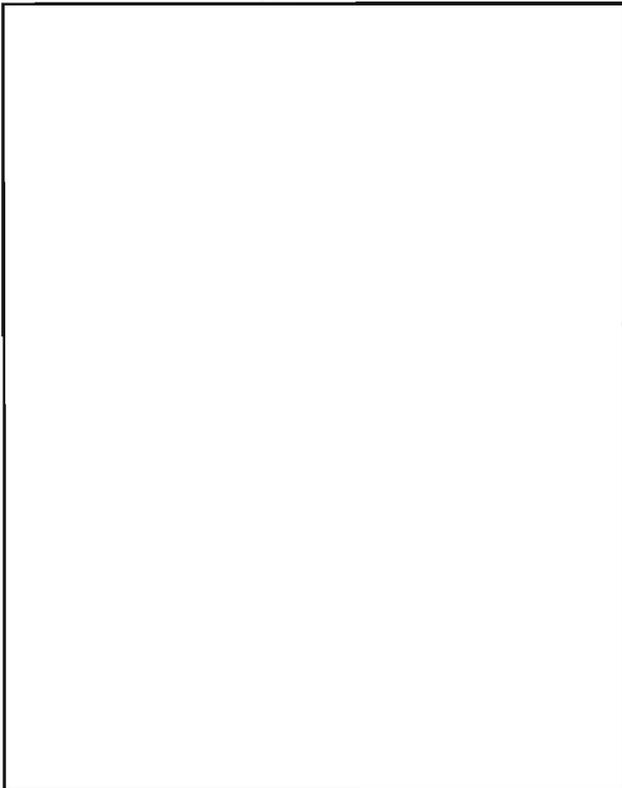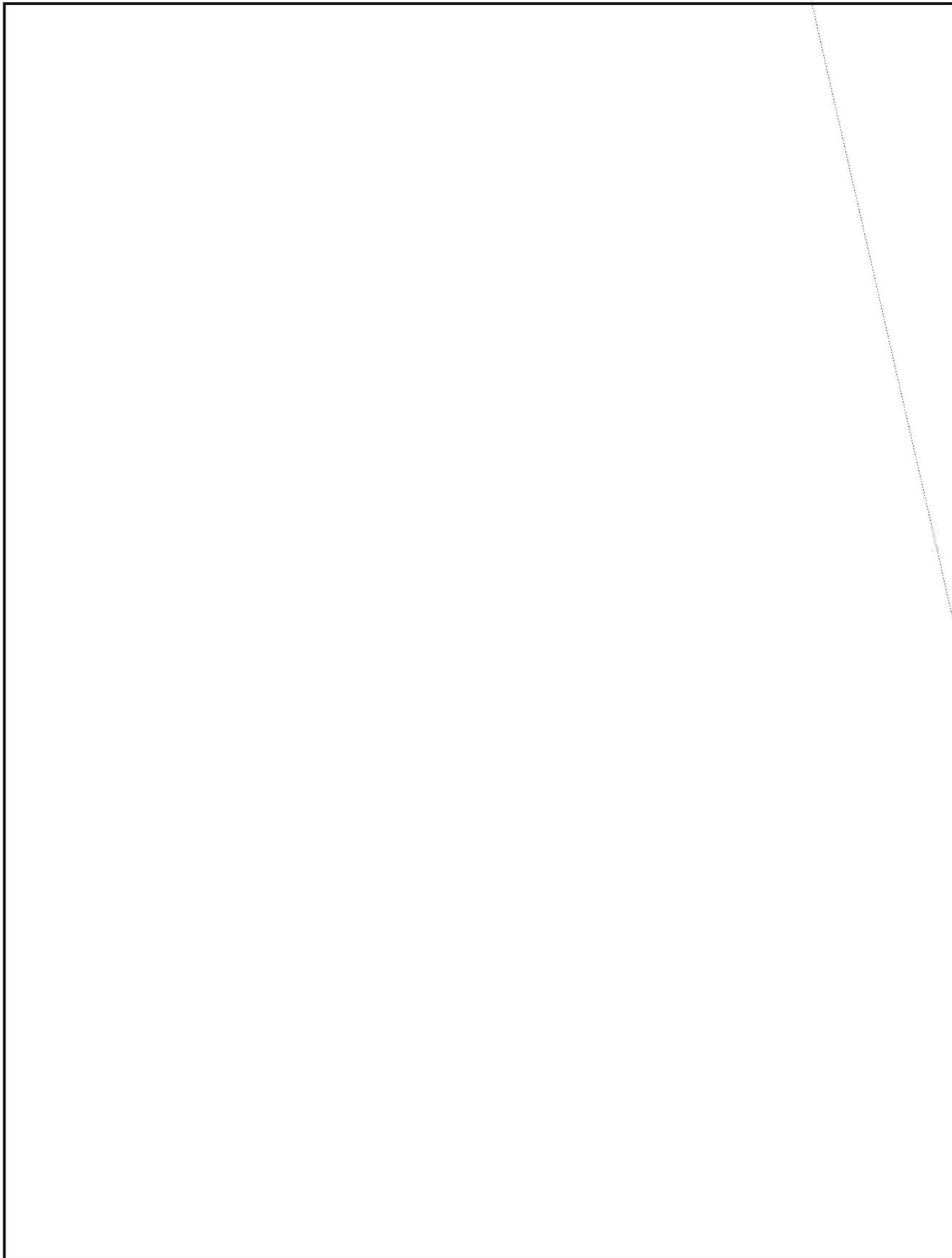
EO 1.4.(c)

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

Information Warfare:

A New Business Line for NSA

by [   ] G42

P.L. 86-36

(TS-CCO) One of the new buzzwords in the hall-ways these days is Information Warfare (IW). IW is defined as the preservation of the integrity of our information systems from exploitation and corruption by potential adversaries while at the same time exploiting and degrading adversary information systems. At the
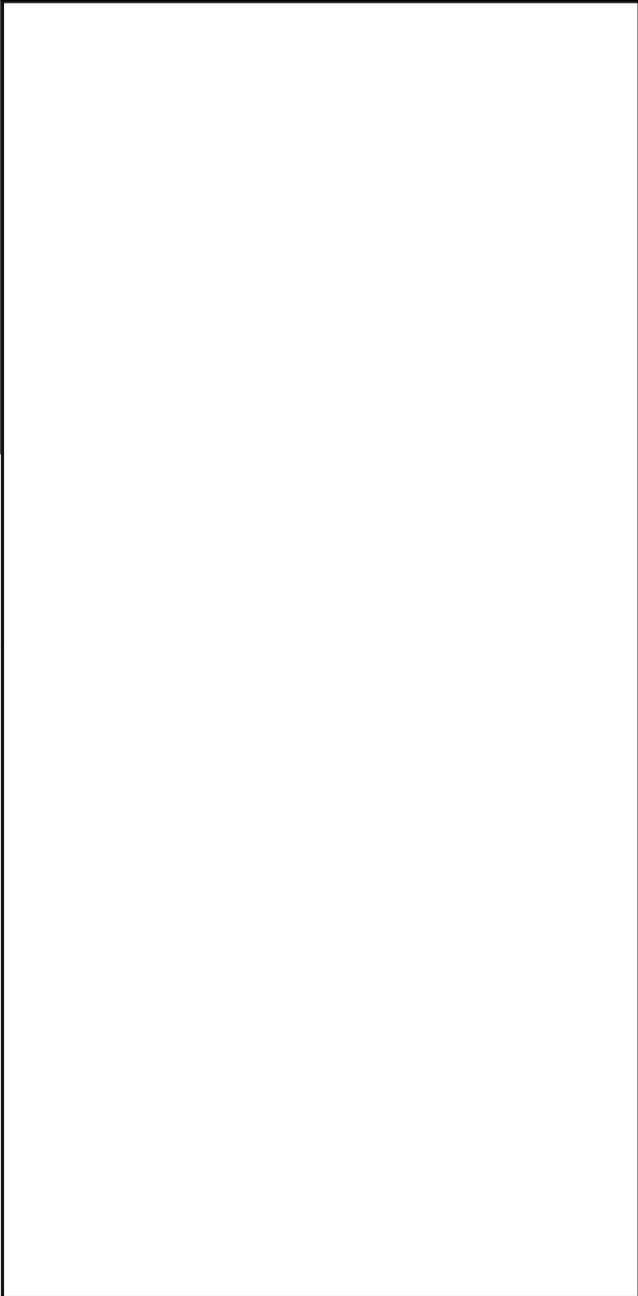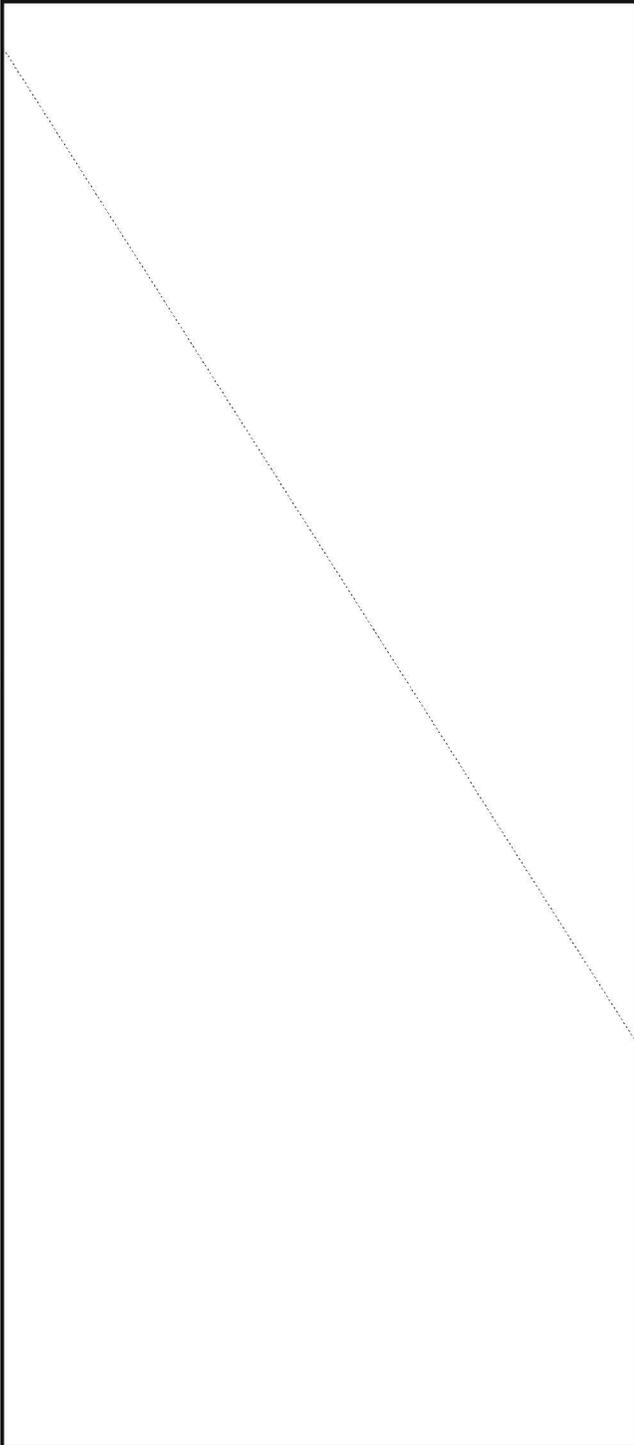
P.L. 86-36

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

(TS-CCO) Information Warfare promises to provide a new way of looking at familiar problems as well as a new set of tools for the war-fighter. NSA will be one of the main players in many future IW developments and our support will be critical to its future.

...and speaking of Information: is anyone going to GIS/LIS '94?

The Geographic Information Systems/Land Information Systems) Annual Conference and Exposition will be held in Phoenix, Arizona from 23-28 October 1994. This will be a multidisciplinary, educational, and scientific meeting designed to foster professional and intellectual interaction among individuals and groups interested in the design and use of GIS, LIS, and related specialties and technologies. The GIS/LIS '94 program will feature the latest ideas, research, and technological advances in GIS, LIS, AM/FM, infrastructure management, surveying, mapping, and related specialties from around the world.

For further information, please contact:

GIS/LIS '94:
5410 Grosvenor Lane, Suite 100
Bethesda, MD 20814-2122

or call: (301) 493-0200
or fax: (301) 493-8245

Please consider writing an article for Cryptolog if you attend this event!

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

CRYPTOLOG
July 1994

Tour of Duty:

P.L. 86-36

by A05

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

5

SECRET SPOKE

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

SECRET SPOKE

HANDLE VIA COMINT CHANNELS ONLY
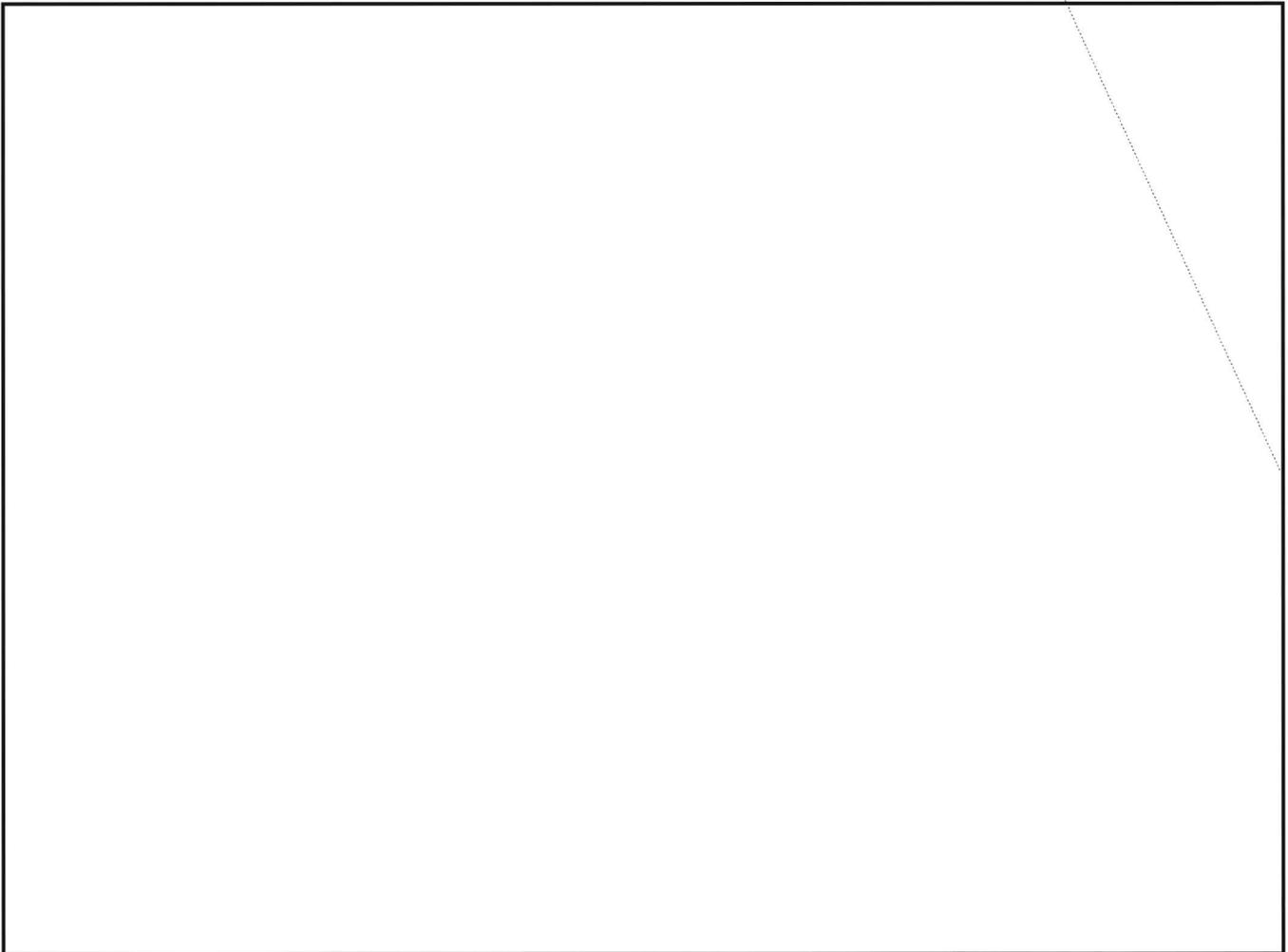
Target Development in the Field

P.L. 86-36

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

by _____

(C-CCO) The purpose of this article is to discuss target development in the field and how it is different from target development as practiced by offices of primary interest (OPIs) at NSA Washington (NSAW). These differences are important for Headquarters analysts to understand, because their ability to work with field target developers will have a direct effect on the product they receive from the field. The ideas in this article are drawn from the author's experience _____ to discuss target development issues, and countless telephone and e-mail conversations with target developers around the world. While these thoughts are not universally applicable, they are valid, in varying degrees, for most large field sites.

(C-CCO) There are probably as many different definitions of target development as there are organizations doing it. One of the problems that arises in discussing the topic is figuring out what is meant by the phrase target development. Since it involves so many different types of activity, there are many different slants on its meaning.

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

CRYPTOLOG
July   1994
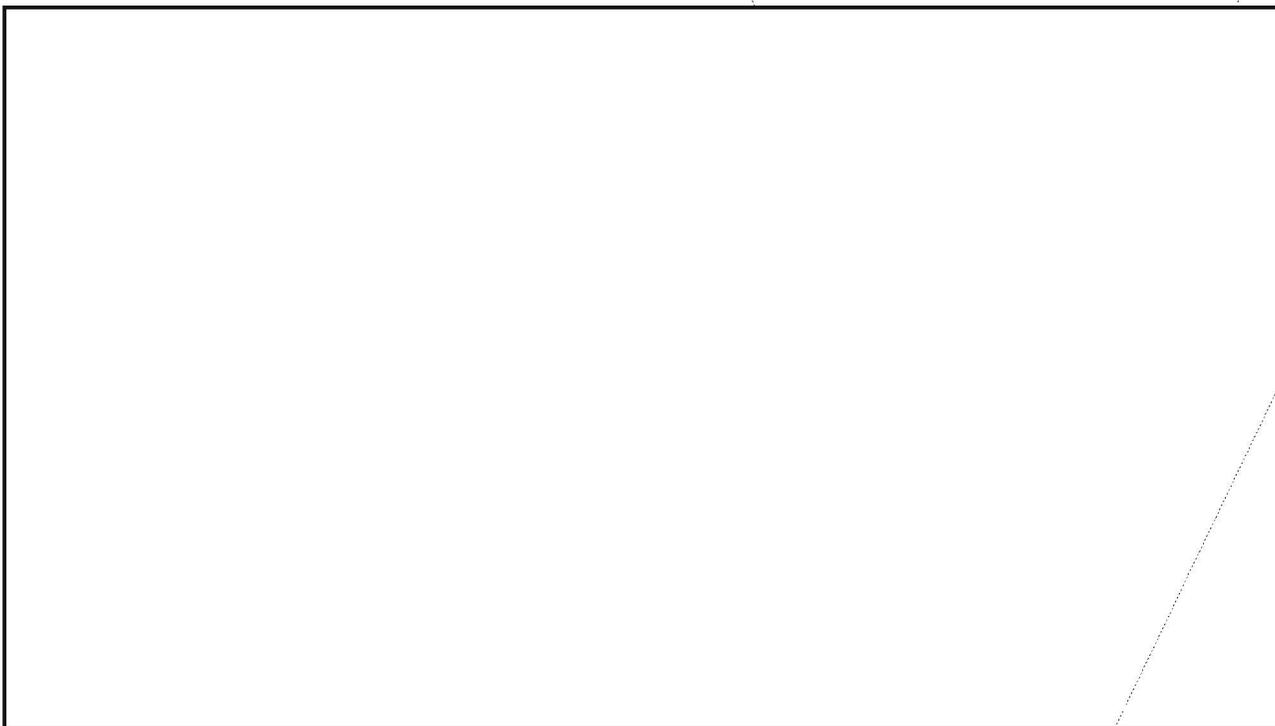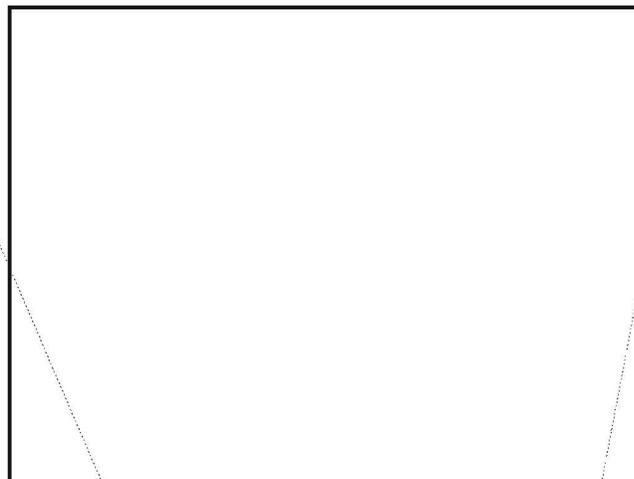
EO 1.4.(c)
P.L. 86-36
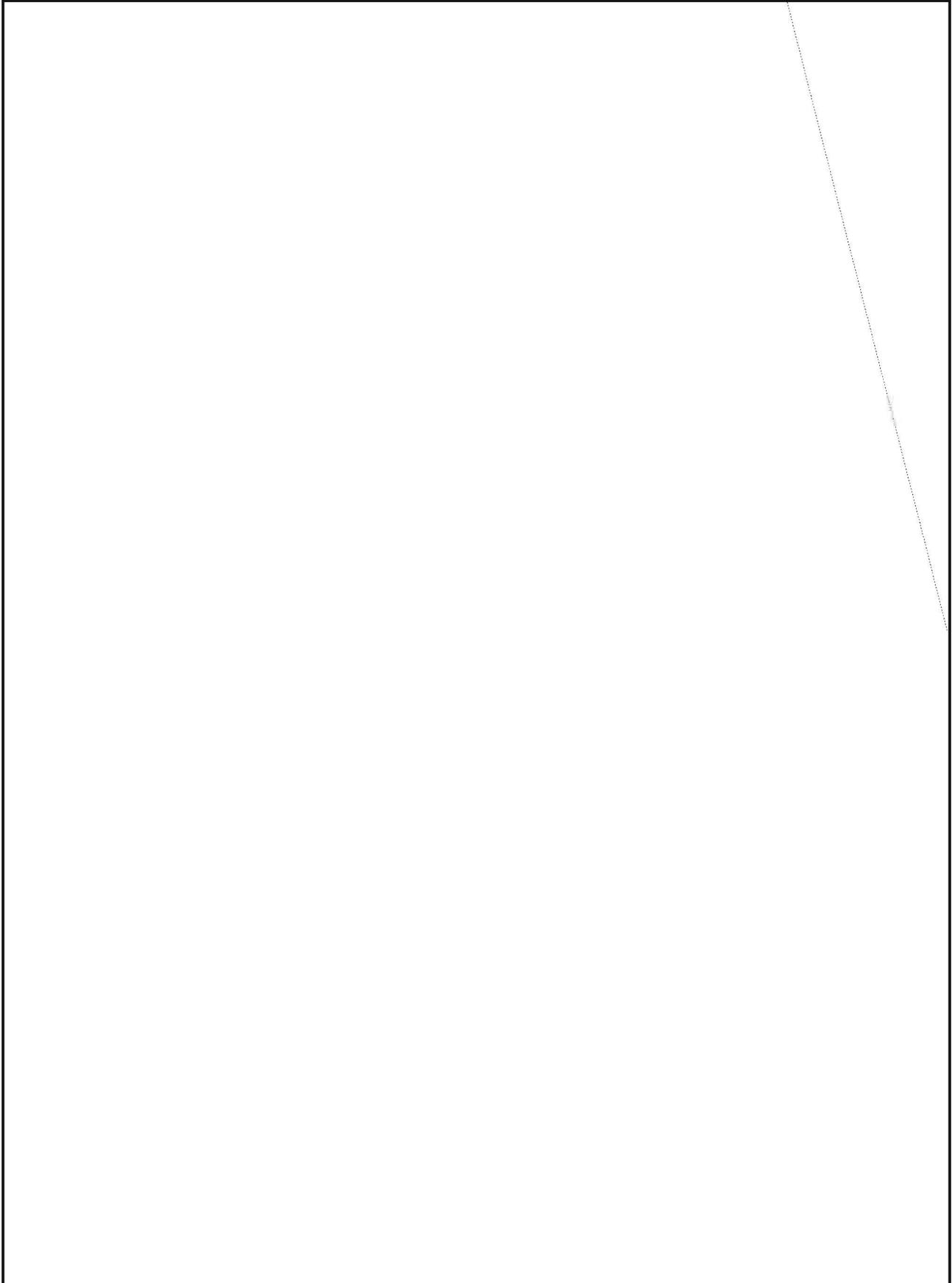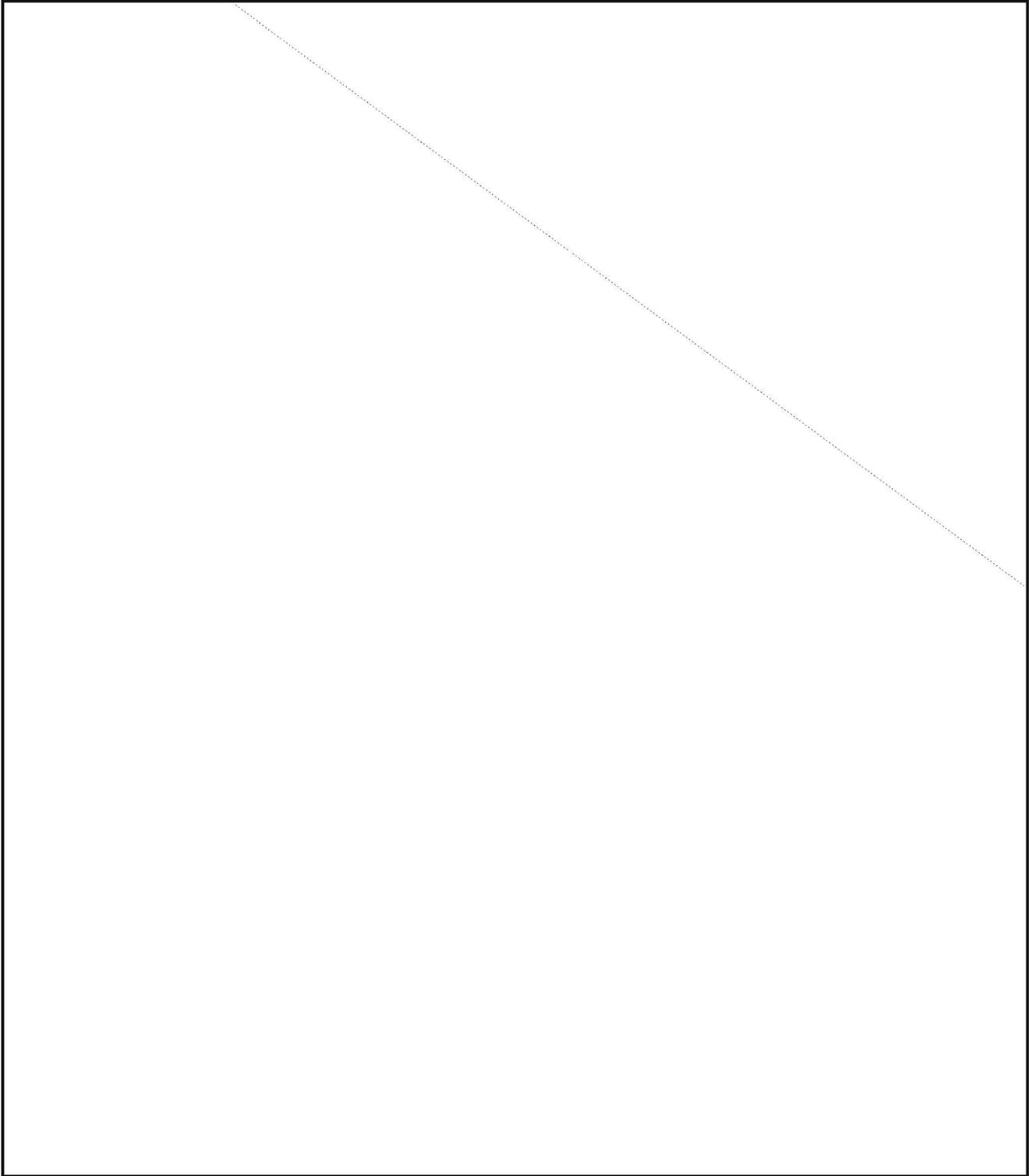
EO 1.4.(c)
P.L. 86-36

P.L. 86-36

Highlights from the Spring SRTD Conference
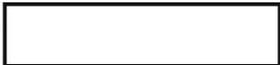
EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

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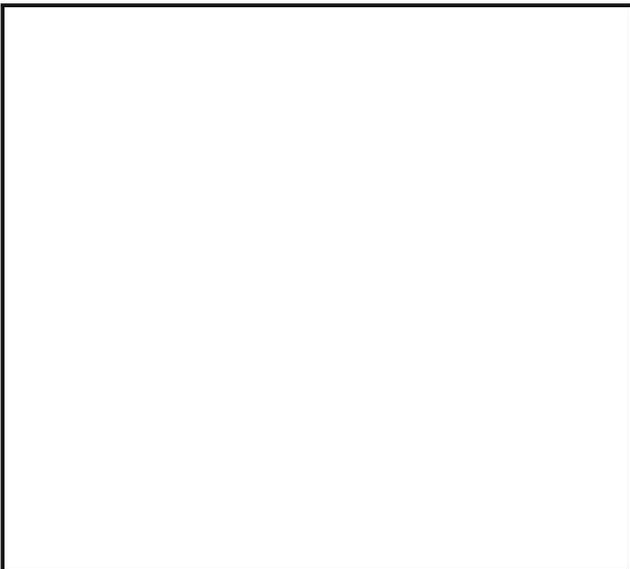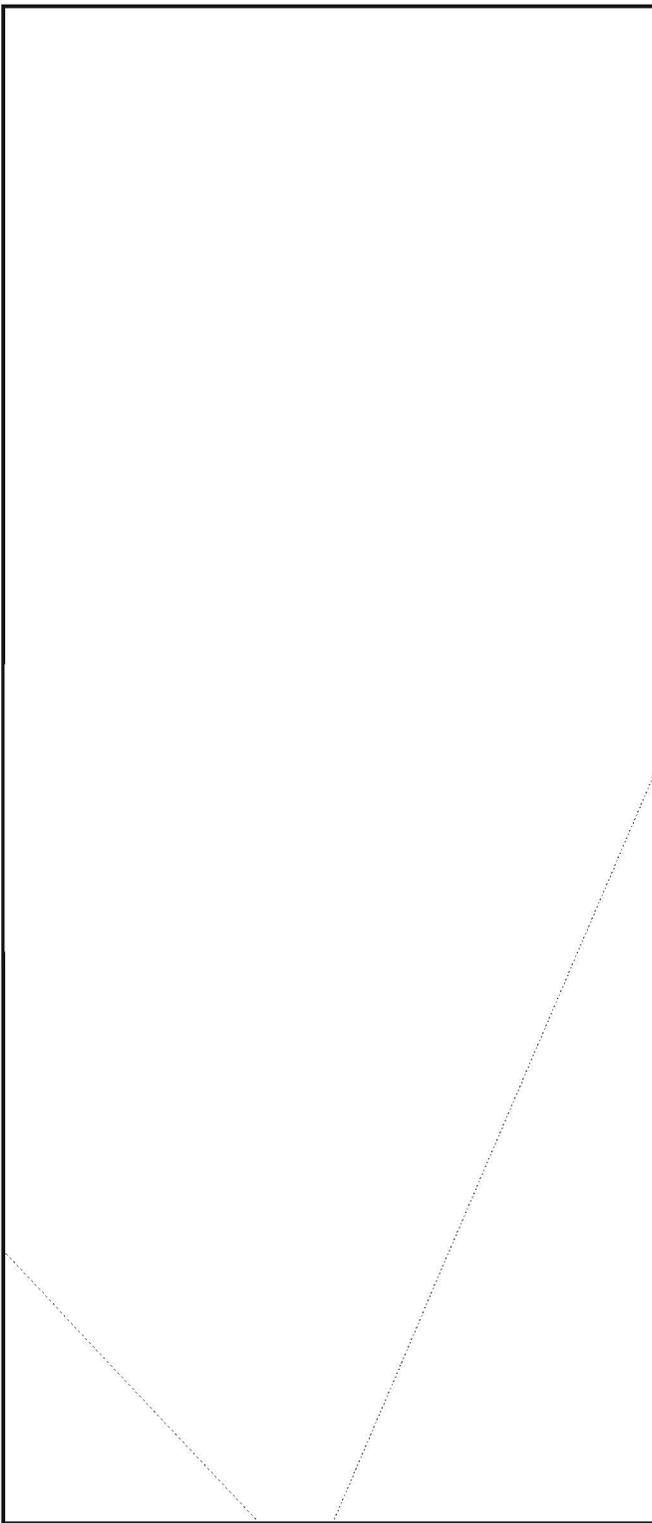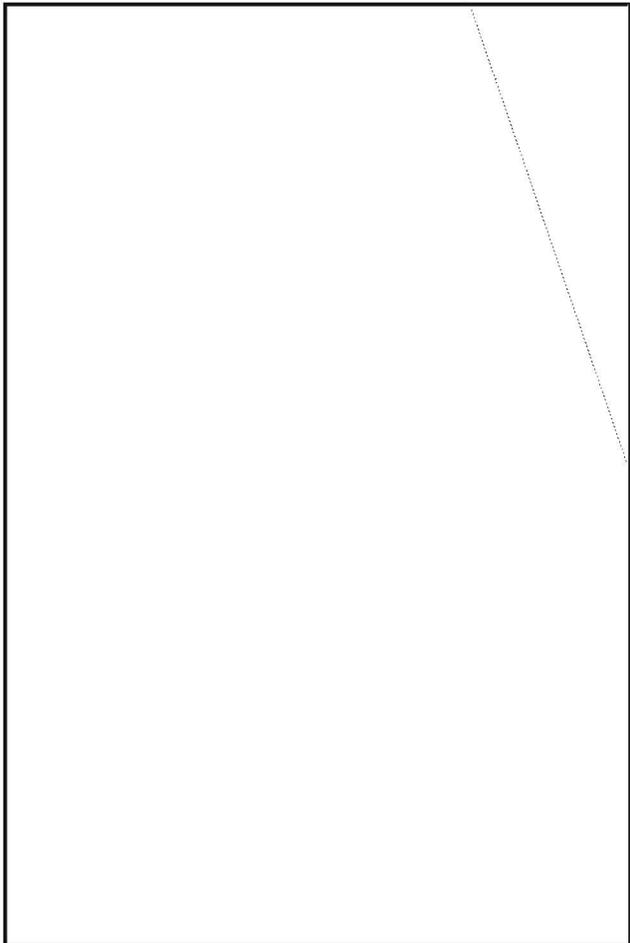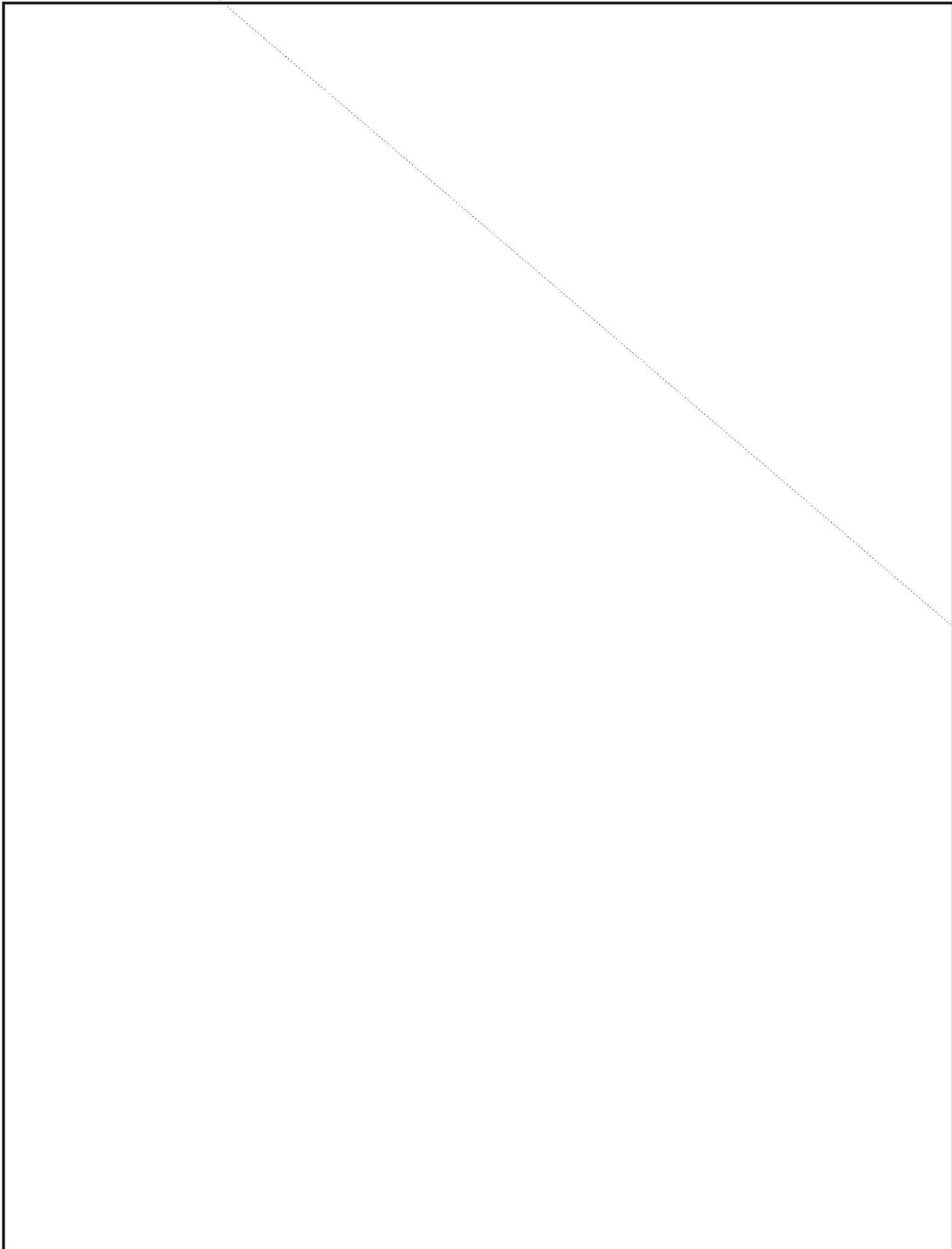
P.L. 86-36

Publishing As A Member Of The Technical Track

by [   ]Y Technical Director

THE PRIMAL NEED TO PUBLISH

(FOUO) The Agency Technical Track Program offers its members an unprecedented opportunity to further their technical skills while growing professionally. Professional growth within the Technical Track is measured by technical accomplishment within three key areas: Performance Factors, Skill Development and Skill Field Contributions. Complete information on these areas can be found in Annex B of NSA/CSS Regulation 32-12, dated 20 August 1993.

(FOUO) Within the area of Skill Field Contributions is a section which establishes the need for members of the Technical Track to publish their work as a vehicle for both technology transfer and career growth. It is upon this aspect of the Technical Track Program that this article focuses.

TECHNOLOGY TRANSFER

(U) What is Technology Transfer (T^2)? It has been defined many ways:

... the process by which technology, knowledge and information developed in one organization, one area, or for one purpose is applied or used in another organization, in another area or for another purpose ... U.S. Department of Energy (1990)

... providing on a timely basis technical information, and assistance in its application, in response to specific, user-identified needs ... J. Wycoff, *Journal of Technology Transfer* (1981)

... a purposive continuous effort to move technical devices, materials, methods and/or information from the point of discovery or development to new users ...J. Gilmore, "The Environment and the Action of Technology Transfer: 1970-1980" (1969)

(U) In general, T^2 may be considered as the overall process of moving technology from its point of origin to its point of need.

WHY DO *I* NEED TO PUBLISH SOMETHING?

(U) The simple answer is that it is now your responsibility as a member of, or an aspirant for, the NSA Technical Track Program. Technical Track members have a professional obligation to ensure that the transfer of technology happens. One of the best, and most long-lasting, ways to accomplish this is to simply share knowledge in written form. Having done this, many future opportunities may arise to expand upon that which has been shared. Such opportunities may be delivering papers at conferences and symposia, providing informational briefings based upon the written product, and/or authoring a sequel document to further enhance a good idea. The possibilities are virtually without limit.

BUT I'VE NEVER PUBLISHED ANYTHING BEFORE

(U) Ignorance is no excuse for the law! Sound familiar? Don't worry, the Technical Track police aren't going to "collar" you for simply not being aware of how to go about getting something published. If anything, you'll probably find so much help and assistance that you'll wonder why you ever had any hesitation about becoming an author in the first place. The main point is that you can, and will, find a wealth of resources to aid you in your personal quest to share your unique technical talents. Try asking a member of the Technical Track who has already published something and see how enthusiastic he/she will respond to your request for information. If we all follow the chain-letter principle (everyone tell two people—and they tell two people, etc.), we'll be knee-deep in "best sellers."

(U) Don't be bashful about asking for help. Remember, the Technical Track also means mentoring is alive and well.

OK, SO I WROTE IT - NOW WHAT?

(U) Now we're talking! The hard part is done. At this point, spend a few extra minutes reviewing your manuscript for both its technical content and attention to detail (spelling, grammar, punctuation, style, etc.). Don't forget to use the built-in power of document-processing software to assist you with the attention to detail part.

(U) It's always a good idea to have a few friends provide you with constructive feedback on your creation. Run it up the flagpole (as they say) and see who salutes. Synergy works and is a proven component of success. Don't be afraid to expose yourself to this peer review process; that's what the Technical Track is all about in the first place: people helping people.

WHERE CAN I PUBLISH MY ARTICLE?

(U) The places to publish are everywhere. Are there any journals which regularly come across your desk or to your computer screen? How about Newsletters and other local publications that you've seen? Most Agency technical societies solicit papers on an annual basis for essay contests; look for the announcements or contact one of the society's officers. How about an organizational technical report that carries a wide distribution? Career Panels and Technical Directors can also help point you in the right direction.

(U) Don't forget unclassified commercial publications which may be appropriate for your document. After an Agency publications review, you've got a whole world out there just waiting for your brilliance.

(U) As an aid to aspiring authors, the Appendix of this article lists a few places where you can get started with your publishing career, along with publishing criteria and initial points of contact.

CONCLUSION

(U) Publishing is simply a state of mind. Be positive about your technical contributions and look for opportunities to share them. Too many people have the misimpression that nobody will be interested in what they write about. At this Agency, nothing could be further from the truth. Everyone can make a significant contribution to the overall level of awareness of the Agency's population.

THE BOTTOM LINE

Publishing articles, reports and/or papers has a lot in common with driving a stick-shift vehicle. At first it takes a lot of effort, but over time, it simply becomes hard to imagine doing it any other way.

P.S. It's also a great feeling to see your name in print!

POTENTIAL PUBLICATION SOURCES

The DD Eye

Editors:
972-2506
972-2666s

P.L. 86-36

Mission

(FOUO) *The DD Eye* Newsletter is published monthly to disseminate information throughout the INFOSEC community. The primary focus of *The DD Eye* is to inform and motivate personnel, increase their knowledge, and improve their performance. *The DD Eye* contains information about Corporate philosophy, organizational missions, career and personnel matters, unique training opportunities and programs, and facilities. The newsletter allows individuals and organizations to share accomplishments with the ISSO work force.

Preferences

(U) Unclassified, short articles that are of interest to the entire work force. Can be technical, but should be written so that non-technical personnel can understand. Will accept classified articles, but they must be classified by the originator. Photos, diagrams, clip art, etc. are encouraged. The author should be identified.

Submitting Items

P.L. 86-36

CRYPTOLOG
July   1994

P.L. 86-36

INFOSEC Technical Exchange

Publisher: [   ] Y272, 972-2102s
Editor [   ] Y221, 972-2406s

(U) The following guidelines should be used in writing an article for the *INFOSEC Technical Exchange*. These guidelines are intended to help a prospective author focus his/her efforts toward an article which meets the spirit of the *Exchange*. We invite all members of the INFOSEC Community to submit articles.

Topics

(U) Articles may address any topic which is of interest to a wide range of INFOSEC professionals. All articles should be:

(U) Relevant, topical, and contribute to the advancement of the INFOSEC Community.

(U) Timely, although historical articles may occasionally be used.

(U) May or may not be highly technical; however, if the topic is highly technical, pay particular attention to the CONTENT guidelines below.

Content

(U) All articles should be of a professional nature and serve as a technical resource for the INFOSEC Community.

(U) Articles may disseminate information on:

* R&D efforts,
* findings from general research,
* recent developments in policy which have a broad impact,
* new achievements in ongoing projects

(U) Articles may introduce a new project or program that needs support from or offers support to a wide range of organizations.

(U) Articles should interest a wide range of INFOSEC professionals.

(U) Articles should be written on a level that will allow all readers to understand the main ideas presented. It is expected that there will be some cases in which highly technical details are essential for a complete article. This is acceptable, as long as comprehension does not depend on a clear understanding of the technical details. In general, technical complexity should be considered the exception rather than the rule.

(U) Classification

(U) The *Exchange* will accept and print articles up to the TOP SECRET level. Each paragraph in a classified document should be properly marked with its classification level (U, C, S, TS).

(U) The *Exchange* is distributed to the branch level in the ISSO and is widely available to NSA employees and others with appropriate clearances for U.S. classified information. Protection of caveated or compartmented information cannot be supported.

Length

(U) Articles should be from one to ten pages long, including any relevant graphs, charts, diagrams, or schematics. If an article is longer than ten pages, the author may contact the publisher of the *Technical Exchange*, for a discussion or advice.

Format

(FOUO) FrameMaker format is preferred. J334 has a conversion service that converts Interleaf, Word Perfect, Office Writer and MS Word into FrameMaker. Just attach the document to an E-Mail Compose Window addressed to **convert@po**. In the message window, type:

Target: FRAME

Send it. The document will be converted and returned to you.

(U) Classify all paragraphs.
(U) Do not double-space between lines.
(U) Do not type your article in capital letters.
(U) Include your name, organization, building, and phone number.
(U) Do not type your article in multi-columns.

Submitting Items

(U) All articles must be reviewed and approved by the writer's organization.

(U) All articles must be approved for publication in the *INFOSEC Technical Exchange* by the Publisher and member(s) of the Selection Panel, who reserve the right to edit, abridge, or refuse to publish an article.

P.L. 86-36

P.L. 86-36

NSA Cryptolog

Publisher: William M. Nolte, P054, 963-3123
Editor: ☐ P054, 963-3123s

Preferences

(U) Classified, technically-oriented articles with emphasis on improving NSA's technical performance; should be aimed at explaining one's discipline to those outside it. Readers are also invited to contribute conference reports and reviews of books, articles, software, and hardware that pertain to our missions or to any of our disciplines. Humor is welcome, too. Submissions may be published anonymously, but the identity of the author must be known to the editor.

Submitting Items

P.L. 86-36

(FOUO) Send a hard copy accompanied by a labelled diskette to the editor at P054 in 2E062, Ops. 1, or ☐

Guidance

* Do not type your article in capital letters.
* Classify all paragraphs.
* Label all diskettes, identifying hardware (OS: DOS, UNIX), density and type of word processor used.
* Put your name, organization, building and phone number on diskettes.
* FrameMaker format is preferred; ASCII is also fine. J334 has a conversion service that converts Interleaf, Word Perfect, OfficeWriter and MS Word into FrameMaker. Just attach the document to an E-Mail Compose Window addressed to **convert@po**.

Information Categories

Collection
Cryptanalysis
Cryptolinguistics
Information Resources
Information Security
Intelligence Analysis
Intelligence Community
Linguistics
Mathematics
Research & Engineering
Science & Technology
Traffic Analysis

Virtual Campus (VC) Advances

Editor: ☐ Y471, 972-2355s

P.L. 86-36

Mission

(FOUO) *VC Advances* is published bi-monthly to promote and publicize Virtual Campus (VC) throughout the Information Systems Security Organization (ISSO). *VC Advances* contains information about Virtual Campus goals and objectives; helpful hints and tips for new VC users; updates on new products and changes; and technical information for our more technically oriented readers. This newsletter gives the ISSO workforce an opportunity to learn about what is coming, voice their concerns, and contribute their expertise.

Preferences

(U) Unclassified, short articles that are of interest to the entire DDI work force. It is preferred that technical articles be written so that non-technical personnel can understand, but that is negotiable, depending on content. (Articles containing important technical information that could benefit at least a part of the work force have been accepted and well-received.) Photos cannot be accepted, but diagrams, clip art, etc. are welcome. Questions and ideas that could lead to articles are also encouraged. The author should be identified.

Submitting Items

P.L. 86-36

Cryptologic Quarterly

Mission

(FOUO) The goal of *Cryptologic Quarterly* is to educate the work force in both narrow technical elements of the cryptologic effort and the broad issues that affect that effort.

Preferences

(U) Articles for *Cryptologic Quarterly* may be written on any theoretical, doctrinal, operational, managerial, or historical aspect of cryptology. The criterion for publication is whether or not the article is of sufficient substance and interest to make a genuine contribution to cryptologic literature. The decision to publish a submitted article rests entirely with the management of *Cryptologic Quarterly*. The author should be identified.

Submitting Items

(FOUO) Contributions should be submitted to [   ] [   ] Managing Editor, *Cryptologic Quarterly*, E324 [   ] 968-6158s.

(U) Manuscripts should be accompanied by an abstract and should be typed double-spaced with generous margins. Two copies are required; a third copy should be retained by the author. Illustrations should be submitted with the manuscript and should be adequately identified. If your manuscript was prepared on a desktop computer/word processor, please submit a disk with the following information: the type of equipment, the operating system, and the word-processing software that you used. All material used in the publication of an article is destroyed when no longer needed unless the author requests that it be returned.

P.L. 86-36

OPSEC In The Post-Cold War Era

by [   ]   P.L. 86-36

(U) As the world settles into the post-Cold War period, the government of the United States finds itself in the awkward position of having no easily identifiable "enemy" at which to point a finger. The threat to our national security, or at least the way we perceive it, has undergone radical changes, yet these changes have only just begun.

(U) To compound the difficult situation faced by our government, we are also in the grip of a budget crisis. Every dollar spent is being carefully scrutinized, with an eye towards "return;" if there is no identifiable benefit from the expenditure of funds on a particular initiative, then the funds will probably be invested elsewhere. Within the Intelligence Community, the "traditional security" measures that have been ritualistically adhered to under the specter of the Soviet Threat have begun to come under question. The question that is being asked, and rightly, is "What is the return on my investment of security dollars?"

(U) In understanding the new concern about the effectiveness of security measures, a word needs to be said about the changing nature of the threat to the Nation's secrets. In the past, there were scores of identifiable cases of espionage. At the height of the Cold War, the Soviet bloc countries had perfected a staggering array of espionage techniques that would enable them to access the guarded secrets of the United States and its western allies. These techniques included sophisticated electronic eavesdropping operations, massive SIGINT and IMINT collection efforts, and the most formidable HUMINT collection network in the world. All of these threats have undergone radical change in the last few years (to say they no longer exist, however, would be a grave error), but the most noticeable change has been in the area of HUMINT operations.

(U) At the height of the Cold War, the Soviets were effectively operating a "closed society," for which we had to develop our own methods of penetration. The United States attempted to make collection of information equally difficult for the Soviets by blanket classification of any and all information dealing with the national security. The Soviets responded with the intelligence collection assets mentioned above, with a particular emphasis on HUMINT. They seemed to like

UNCLASSIFIED

HUMINT collection, and they were good at it, perfecting a seemingly endless array of techniques for surreptitious entry, penetration of security containers, access to restricted areas, co-opting of trusted employees, illegal agent operations, and other means of "sneaking around." To make matters worse, at least in the mid-1980s, there seemed to be a fairly large number of Americans who were seeking out the Soviets or any other foreign government to which they could voluntarily provide sensitive or classified information. From what we were able to discern at the time, it was apparent that investments in "traditional security," i.e. safes, locks, fences, guards, badges, strict classification policies, TEMPEST countermeasures, etc., were money well spent.

(U) Today, however, we find ourselves dutifully adhering to security policies and procedures that were effective and prudent during the Cold War, but whose effectiveness has been reduced or eliminated. Blind adherence to these policies at times may even impede mission effectiveness, and the justification to continue to spend money on these measures is increasingly difficult to accept. The reason is that many of these security measures are no longer protecting our information. Our adversaries have found that there are more economical

The dawn of the "information Age"....has changed the concept of protection of information...we can no longer "protect it all."

ways of obtaining information that do not involve "sneaking around;" instead, they need only sit down at a computer terminal, visit a library, or submit a request for (unclassified) information to the Federal Government. These methods, unthinkable in the Cold War world of 15 years ago, have been made possible by another phenomenon—the dawn of the so-called "Information Age."

(U) Within the last 10 years, technology advances have changed the way in which we view information. We now literally have the world at our fingertips, with access to worldwide networks and databases that contain virtually every piece of information available. This has also changed the concept of protection of information. What we once protected easily by lock and key is now being transmitted worldwide at the speed of light. This has led us to the realization that we can no longer protect it all. Instead, we need to determine what the truly critical pieces of information are and develop a carefully orchestrated strategy for their protection. The

means by which we identify, and subsequently protect, this information forms the discipline of operations security, or OPSEC.

(U) OPSEC is a five-part process (and I say "five-part" rather than the more familiar "five-step" to avoid the suggestion that the five parts occur in a particular sequence). These five parts are:

- **identification** of critical information
- assessment of **vulnerabilities** associated with that information
- assessment of **threats** to that information
- assessment of the risk that the information will be **compromised**
- implementation of **countermeasures** to prevent compromise of the critical information

---

(U) OPSEC is an analysis of the flow of information, from an adversarial perspective, and the informed application of countermeasures based on that analysis.

(U) In today's world of budget constraints, the risk analysis phase takes on particular significance. Risk analysis means assessing the probability that a particular source of information will be successfully exploited by an adversary. For example, if a determination is made that a vulnerability exists for a particular item of information, but there is no demonstrated threat to exploit that vulnerability, then the overall risk is low. A similarly low risk factor would be assigned to information to which a known threat was posed, but with which no vulnerability was associated. In other words, the expenditure of significant funds to protect that information would not be justified. Also critical to the risk analysis phase is the concept of "value of information." The cost of protecting the information in question should not exceed the intelligence value of that information. It is in this way that OPSEC can be seen as an effective cost-saving tool; it identifies the areas in which limited security resources can be put to their best use. OPSEC can identify areas in which existing, and sometimes costly, security measures are not effectively protecting the information they were intended to protect, and can free up those resources to be applied in another area where they will have a greater effect.

(U) This is not to say, however, that the risk analysis phase is the only one of importance. When seeking to protect information, the critical step that is often overlooked is the identification of exactly what needs protection. Adherence to the OPSEC framework forces an

UNCLASSIFIED

identification of that critical information. In today's environment of information exchange, it is simply not possible to protect all information that is associated with a particular program or initiative. Instead, that information which is absolutely critical to the success of a program (the "golden nuggets") must be identified and protected. Along with the identification of exactly what information is critical, a realistic assessment should be made of what, if any, information has already been compromised, or can reasonably be assumed to be known or available in the public domain. *We are currently spending enormous sums of money "protecting" information that has been publicly known for many years.*

(U) In identifying the threat to a particular piece of information, we should be careful not to rely on Cold War threat assessments of what an adversary "could" or "might" ascertain, or what his "probable" or "possible" capabilities are. In today's tight financial times, funds will be increasingly allocated toward defending against demonstrated, rather than postulated, threats. If there is a reasonably good indication that there is a threat to critical information, then countermeasures should be applied to that threat. We can no longer afford, however, to defend against threats that have never been demonstrated. We also need to assess the likelihood of a particular threat. Would an adversary mount a sophisticated, expensive, high-risk SIGINT operation against a particular target if he could get the same information from Nexis-Lexis or a similar database? In most instances, the answer would be no.

(U) The assessment of vulnerabilities that could reveal critical information is an equally important part of the OPSEC process. It may be that existing security measures are adequately protecting critical information, but it is this phase of the OPSEC process that will result in that determination. By reconstructing the flow of information into, through, and out of an organization or project, the OPSEC analyst can identify the vulnerabilities of the critical information independently of security measures that are already in place. It will immediately become apparent whether or not the existing security measures are, in fact, protecting the information in question.

(U) The culmination of the OPSEC process is the identification and application of countermeasures. It is in this area that OPSEC often stands alone as the economical alternative to more traditional (and often costly) security measures, because OPSEC countermeasures are frequently simple administrative changes. These changes can range in scope from the development of a deception plan, to the omission of a few items of information from a shipping label, to the decision not to release a particular item to a local newspaper. OPSEC involves an assessment of existing resources, followed by a subsequent plan of re-aligning these resources to provide the maximum protection for the identified critical information. Occasionally, OPSEC countermeasures will include additional changes that do have a cost associated with them, such as the provision of secure communications equipment, but this is not usually the case.

(U) Viewed in this way, it becomes apparent that **OPSEC can be a valuable tool for cutting costs without sacrificing protection.** By identifying the information that really needs to be protected, OPSEC ensures that this information is safeguarded by relevant countermeasures while eliminating unnecessary and often costly security measures that are oriented toward an undocumented or unlikely threat. Furthermore, if OPSEC is employed throughout the entire life-cycle of a program or system, as it should always be, it can provide further savings in the form of dollars that will not need to be spent re-developing or replacing a system or program that has been compromised even before it is fielded. The intention is not to imply that, in embracing OPSEC, we should throw existing security measures out the window. However, in practicing OPSEC consistently, we can determine which security measures are effective and which ones are not, and in the long run ensure that the dollars we spend on security are doing the most toward protecting our truly critical information.

A Linguist's Look at the Internet

P.L. 86-36

by [ ]

(S) Open-source information (OSI) has grown to enormous proportions in recent years. Communicating electronically has become simple and cheap and, as a result, global information access has virtually exploded. We may be reaching the point where it's impossible to track systems, let alone users of systems. Where in the past OSI was given little attention or even disregarded, today its intelligence potential has grown dramatically. It is being turned to more and more to fill gaps in analysis, to validate intelligence assessments, even to interpret SIGINT and to direct SIGINT tasking. The shift in priority from military to civil targets in particular has placed much reliance on OSI to increase understanding of political, economic, and scientific targets and to keep up with events in those areas. The Intelligence Community has recognized the importance of OSI and the need for a broad-based OS program. As a result, NSA may soon be playing a significant role in the acquisition and exploitation of OSI.

P.L. 86-36

(U) Probably the single largest window into the world of Open Source is the *Internet*. For the past six months, my colleague [ ] and I have been accessing the Internet in search of information, tools, and applications primarily in support of A Group linguists. This article is meant to familiarize linguists with the Internet as a source of unique and timely collateral information. It also describes Internet resources of particular interest to linguists but is not intended as a general guide to the Internet. For some points of orientation I have borrowed from existing literature. For a more complete orientation to using the Internet and for more detailed descriptions of Internet resources, a list of references follows this article.

(U) The A Group Language Technology Center's (ALTC) use of the Internet has been in three general areas:

[ ]

This paper will describe what we've found in each of these areas which we consider of interest to language analysts. Included are sample snippets from messages and documents which we've encountered as well as listings we've compiled of useful resources. We must emphasize that we've only scratched the surface of what the Internet has to offer. The information presented here reflects only six months of "navigating the Net" and is only meant to give a glimpse of the potential of the Internet as a rich source of useful OS information.

I. The Networks

What is an "internet"?

(U) An "internet" is a computer network which allows computers with differing software and hardware to communicate by translating messages to a common *communications protocol*. The first real internet, the ARPANET, was a wide-area experimental network in the mid-1980's which arose from research supported by the Advanced Research Projects Agency (ARPA), now DARPA, Defense Advanced Research Projects Agency. The ARPANET connected terminal hosts and servers together and, as local-area networks grew, many hosts became gateways to other local networks. A network layer to allow interoperation of these networks was developed and called IP (Internet Protocol). Over time, other groups (NASA, NSF, states, etc.) created long-haul IP-based networks. The collection of all these interoperating networks, a world-wide network or networks, is what has come to be called "The Internet."

(U) Allowing simple PCs and sophisticated mainframes to interconnect, the Internet can be used for an extraordinary range of purposes: long-distance collaborations, transfer of programs and documents between remote computers, accessing library catalogs, logging into supercomputers...the list gets longer every day.

(U) The Internet has become so immense and complex that there probably isn't a single person who understands everything about it. It now comprises thousands of networks and hundreds of thousands of connected computers, serving millions of users. More users and services are added every day, making mailing lists, resource guides, etc., out of date almost as soon as they are generated. Despite its enormity and complexity, however, the Internet global village operates under certain common conventions and standards[1], even a certain global "netiquette." Once one has mastered a few basic skills, using the Internet is actually very easy.

---

1. RFCs (Requests for Comment) are documents which form the system of standards adhered to on the Internet.

P.L. 86-36

(U) Before we go any further, we need to define the following essential terms.

Internet:	Simply put, the Internet is a large "network of networks." There is no one network known as the Internet; rather, regional networks are connected into one great living thing, communicating at tremendous speeds with the TCP/IP protocol. All activity takes place in real time.
UUCP:	the UUCP network is a loose association of systems all communicating with the UUCP (Unix-to-Unix Copy Program) protocol. It's based on two systems connecting to each other at specified intervals (a process called polling), and executing any work scheduled for either of them.
BITNET:	The "Because It's Time Network" consists of systems connected by point-to-point links, all running the NJE protocol. Mail gateways are in place to reach users on other networks.

(U) These networks are linked in a variety of ways:
1) dedicated telephone lines with 56Kbps connections,
2) special phone lines with 1Mbps connections,
3) special backbone links which can carry a massive 45Mbps load of traffic.

These links are paid for by each participating institution to a local carrier (e.g., Bell Atlantic owns PrepNet, the main provider in Pennsylvania). Also available are special connections which carry Internet traffic (packets) over high-speed modems.

(U) UUCP links (whose connections are of the store-and-forward variety described above) are made mostly via modem. Also in use are Internet-based UUCP links. Using TCP/IP connections, these links provide some blindingly fast "hops," allowing one to communicate cross-country or around the world for the price of a local phone call.

II. Electronic mail:

(U) Electronic mail (e-mail) is the most common form of communication in computer networking. It allows people to write back and forth without having to worry about how messages actually get delivered. Most Agency users are familiar with e-mail addressing and mail-system protocols, so we won't go into detail here.[1] The same **user@somewhere.domain** convention is used on the Internet; every machine connected has a unique IP address or *dotted quad* (e.g. **147.31.254.103**). The trailing domain is often one of the following:

com	**company or commercial institution**
edu	**educational institution**
gov	**government organization**
mil	**military organization**
net	**administrative host for a network**
org	**private organization**

Each country, in addition, has its own top-level domain (**.au**= Australia, **.ca** = Canada, etc.)

(U) Mail messages also have a specific structure that's common across every type of computer system:

```
From:  clinton@hq.mil Sat Feb 27 17:06:01 1993
Received: from hq.mil by house.gov with SMTP
   AA21901 (4.1/SMI for al@house.gov); Sat,
   Feb 27 93 17:05:56 -0400
Date:  Sat, 27 Feb 93 17:05:56 -0400
From:  The President <clinton@hq.mil>
Message-Id: <9105252105066310hq.mil>
To:  al@senate.gov
Subject:  Meeting

<Text>
```

Note that the first **From:** and **Received:** lines give the "real" address that the mail is coming from (as opposed to the address to which you should reply, which may look very different) and what places the mail went through to get to you. If a message is sent using UUCP there will be a **Received:** line for each system that the mail passed through (unless the mail program filters them out). The second **From:** contains the address to which you would reply as opposed to the address from which the mail was sent..

---

1. The basic format of an electronic mail message on the Internet is defined in RFC0822. For more information on e-mail, see *!%@:: A Directory of Electronic Mail Addressing and Networks*, Donnalyn Frey and Rick Adams, pub. O'Reilly & Associates, Newton, MA, 1989.

SECRET

(U) The e-mail one encounters on the Internet is either that routed via a discussion list or a newsgroup (explained later). The header of a typical e-mail message passed over the Russian Electronic Communications network (RELCOM, sort of the Russian equivalent of our PRODIGY service) would look like the following (after converting the Cyrillic for proper display):

```
From newcom.kiae.su!L-relcom@newcom.kiae.su Sun
        Feb 28 08:50:28 1993
Return-path: <newcom.kiae.su!L-
        relcom@newcom.kiae.su>
Received: from techno.fuug.fi by
        afterlife.nscs.mil (4.1/SMI-4.1)
        id AA19408; Sun eb 28 08:50:22 EST
Received: from newcom.kiae.su by techno.fuug.fi
        with UUCP id AA10887
        (5.65c/IDA-1.4.4); Sun 28 Feb 1993
        15:27:56 +0200
Received: by newcom.kiae.su; Sun 28 Feb 93
        15:32:12 +0300
To: subscribers@techno.fuug.fi
Newsgroups: relcom.bbs
From: Alex Popov <alex@mechta.mak.su>
Subject: [News] BBS na Iskre II
Date: Fri, 26 Feb 93 20:55:28 +0300
Organization: A&B Net (A&B_Net_gate)
X-Gate: UU2 1.13b
Sender: L-relcom@newcom.kiae.su
X-Class: Big/nPrecedence:junk
Status: RO
```

This is a message uploaded to a newsgroup (**rel-com.bbs**) announcing a new **A&B Net** BBS being set up at **Iskra II** (International). **Newcom** is the news server for the RELCOM network based at **kiae** (Kurchatov Institute of Atomic Energy). Note that this message has been relayed through a European Internet node in Finland (**.fi**). Note also the exclamation point in the address (**newcom.kiae.su!...**). E-mail addresses usually appear in one of two formats: an "at" sign (**@**) for the Internet format or a "bang" (**!**) for the UUCP format. In addition, a percent sign (**%**) often acts as an extra routing method indicating a specific gateway to another network:

user%site.bitnet@bitnet-gateway

For example:

ukraine%indycms.bitnet@pucc.princeton.edu

is the Internet address for recipients of the BITNET discussion UKRAINE. This list is moderated from a host at Princeton University (**pucc**) via the BITNET node **indycms**.

UUCP Maps

(U) The UUCP Mapping Project at Rutgers University is an attempt to manage the growing number of UUCP hosts. UUCP "maps" allow mail routers within UUCP to work properly. The map for a domain is processed by a program called **pathalias** which generates UUCP routes from the data. The map data is in the following format:

```
#N          UUCP name of site
#S          manufacturer machine model; OS &
            version
#O          organization name
#C          contact person's name
#E          contact person's electronic mail
            address
#T          contact person's telephone number
#P          organization's address
#L          latitude/longitude
#R          remarks
#U          netnews neighbors
#W          who last edited the entry; date
            edited
sitename    .domain
sitename    remote1 (freq), remote2 (freq),
            remote3 (freq)
```

The UUCP map for Russia (domain name **.su**), thus essentially contains a database of information about Russian e-mail subscribers to the Internet. For example:

```
#N          ihep.su
#S          VAX-11; ULTRIX
#O          Institute for High Energy Physics
#C          Leonid Yegoshin
#E          egoshin@ihep.su
#T          +7 (Serpukhov) 42952
#P          IHEP, Serpukhov SU-142284 Moscow
            District, Russia
#L          37 10 E / 54 55
#R          The main relay server of local nets
            on the territory of IHEP
#W          egoshin@serp.ihep.su 910215,
            any@hq.demos.su 910708
```

The **ihep.su** server connects other users listed in the map, such as **serp.ihep.su**, which happens to be an IBM PC/AT running XENIX. It's easy to see how useful these maps can be in tracking systems, users of systems, and organizations. UUCP maps are available by *anonymous ftp* (explained below) from **ftp.uu.net** in subdirectory **uumap**. The map for Russia (actually ex-USSR) is in files **u.sun.0,1,2,3,4,100**. A separate map for the Ukraine is in file **u.ukr.1**. These maps were last updated in December 1991.

SECRET

CRYPTOLOG

Mailing and Discussion Lists

(U) People that share interests are inclined to discuss hobbies or interests at every available opportunity. One modern way to aid this exchange of information is by using a *mailing list*, usually an e-mail address that redistributes all mail sent to it to a list of addresses.

(U) There are two general types of mailing lists: 1) those moderated by individuals to whom you should direct inquiries about joining the list, and 2) those open to public access.

(U) An automated mail-list system called *listserv* allows all the functions of adding and removing users to and from a list to be performed under program control. Recent versions of listserv also provide file-server functions which allow moderators to make data files available to subscribers.

(U) Each discussion list run from a listserver has two e-mail addresses. You send commands to the listserv address and messages to the group address. For example, RUSTEX-L is a discussion list maintained at the University of Buffalo concerning the Russian version of TeX, other Russian text-processing systems, thesauri, spell-checkers, keyboards, etc. If you can send and receive Internet mail, you can subscribe to RUSTEX-L by sending the following message to **listserv@ubvm.cc.buffalo.edu**:

sub rustex-l your_full_name

where **your_full_name** is your REAL name and NOT your network user ID. Once your subscription is acknowledged, you can use other commands to learn more about the list:

index rustex-l	sends a list of available archive files
info genintro	retrieves General Information Guide
review rustex-l	returns the network address and names of all subscribers

You can then send mail to the list by using **rustex-l@ubvm.cc.buffalo.edu** as the group address and everyone on the list will get your message.

(U) For some lists, administrative tasks are handled with the suffix **-request**. NL-KR-L, for example, is a discussion list on natural language processing and knowledge representation maintained at the Rensselaer Polytechnic Institute. To join the list, one would send the "subscribe" command to the following address:

nl-kr-l-request@cs.rpi.edu

A number of mailing lists are set up not as discussion lists, but as a means of distributing newsletters, digests, reports, bulletins, etc. SUEARN-L, for example, carries a monthly digest on ex-USSR connectivity with the Internet. Many sites channel such digests into newsgroups or similar systems which let many users read a single copy of the digest. If such access is available, reading such a "public" copy is preferable to having your personal copy e-mailed to you (saving some network bandwidth!).

(U) Needless to say, listservs have become extremely popular. The latest issue of "The Eastern European list of Electronic (Computer-Accessible) Resources," for example, contains 124 discussion lists just relating to East European issues. There is even a list (**mailing-lists@ijs.si**) whose sole function is to publish a monthly directory of South Slavic mailing lists.

(C) The ALTC has been sampling a significant number of discussion lists to gauge the nature of their content and usefulness (see following listings). So far we have remained passive observers, refraining from any active participation in discussions. We can see the benefit, however, of two-way contact now and then with other language professionals on certain topics. This is permitted as long as users are careful not to reveal Agency need, interests, or capabilities.

CRYPTOLOG
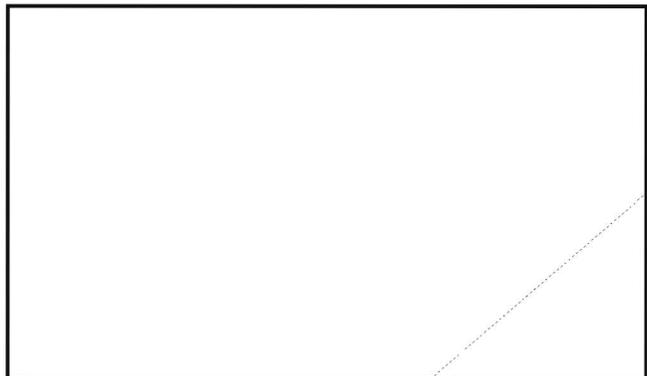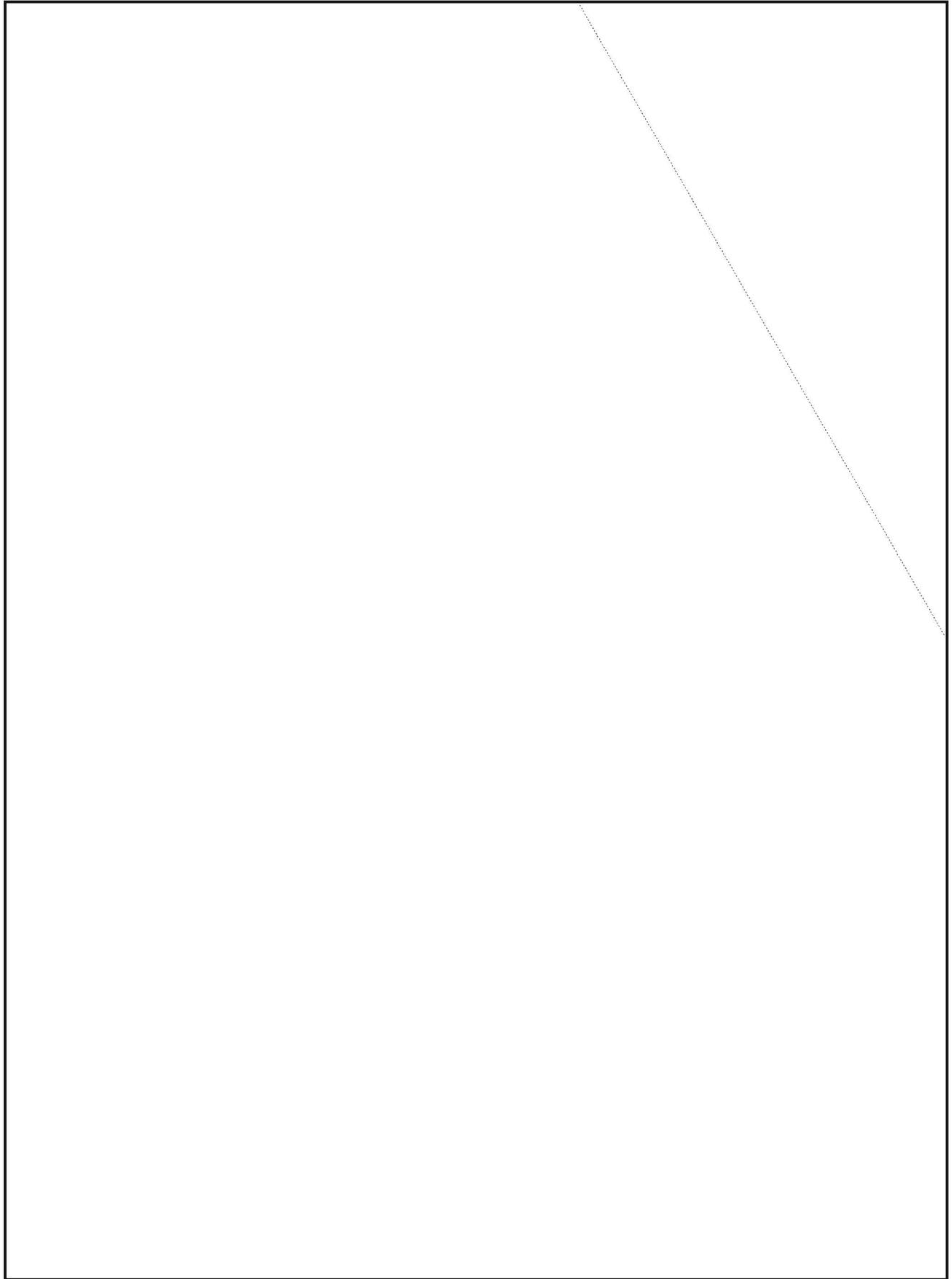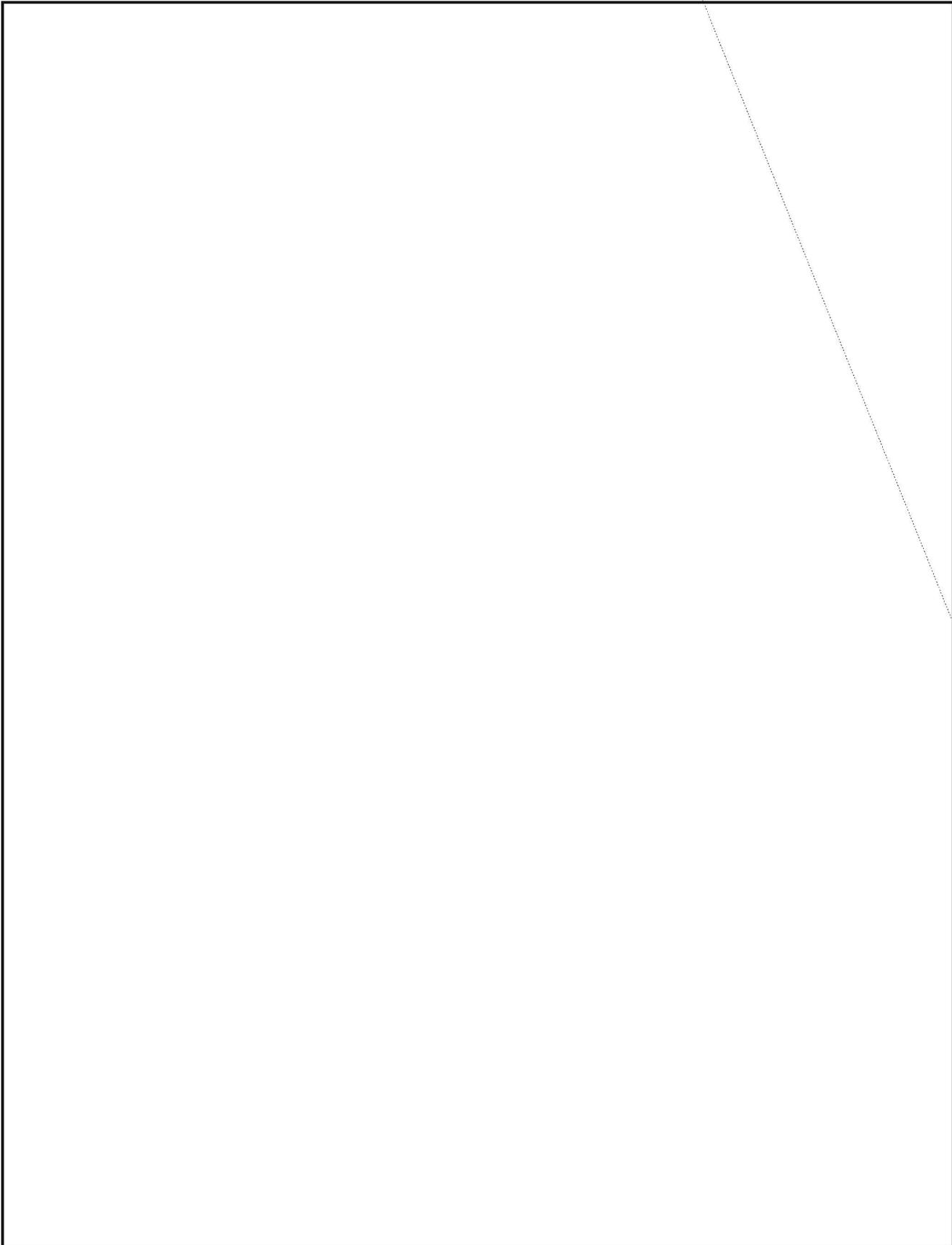
General Guides to Using the Internet

(U) The following are useful as introductory and general guides to using the Internet. A more comprehensive list of recent Internet books can be found in RFC #1432 by J. Quarterman, Mar. 93, available on-line by anonymous ftp from **nic.ddn.mil** in subdirectory **/rfc** as file **rfc1432.txt**.

• *Zen and the Art of the Internet: A Beginner's Guide to the Internet, 2nd ed.*
Brendan P. Kehoe, Prentice-Hall, 112 pp., $22.00. Probably the shortest of the introductory books. The on-line first edition, dated Jan 92, 96 pp., is available by anonymous ftp from **ftp.cs.widener.edu** in the **pub/zen** subdirectory as file **zen-1.0.ps**.

• *The Whole Internet User's Guide and Catalog*
Ed Krol, O'Reilly & Associates, Inc., Sebastopol, CA, 376 pp., 13 Sep 92, $24.95. Aimed more at graduate students who want to use the Internet for research. Ed's 1989 paper *The Hitchhiker's Guide to the Internet*, 22 pp., is available on-line by anonymous ftp from **uxc.cso.uiuc.edu** and other sources.

• *The Internet Companion: A Beginner's Guide to Global Networking*
Tracey LaQuey, Addison-Wesley, 196 pp., $10.95. Aimed at the general public. Being made available on line, two chapters per month, for anonymous ftp from **world.std.com**.

• *Internet: Getting Started*
April Marine, SRI International, 333 Ravenswood Ave., Menlo Park, CA; 380 pp., Sep 92, $39.00. How to join the Internet, and some context so you will know why. Neither a guide nor a catalog, but contains numerous contact listings.

• *The Internet Passport: NorthWest/Net's Guide to our World OnLine, 4th ed.*
Jonathan Kochmer and NorthWestNet, Bellevue, WA, 450 pp., 1993. On-line version, *Internet Resource Guide*, 3rd ed., Oct 92, 300 pp., is available by anonymous ftp from **ftphost. nwnet.net** in **nec/nwnet/user-guide** subdirectory, file **nusirg.whole-guide.ps.Z**.

• *The New User's Guide to the Internet*
Daniel P. Dern, McGraw-Hlll, New York, 1993.

• *An Internet Primer for Information Professionals: A Basic Guide to Networking Technology*
Elizabeth S. Lane and Craig A. Summerhill, Meckler Corp., Westport, CT, 200 pp. 1992, $37.50.

• *Crossing the Internet Threshold: An Instructional Handbook*
Roy Tennant, John Ober, Anne G. Lipow, foreword by Clifford Lynch; 142 pp., 1993, $45.00. A short textbook on using the Internet, by two librarians at the University of California at Berkeley.

• *CICNet Resource Guide*
Available by anonymous ftp from **nic.cic.net** in subdirectory **pub**, file **resourceguide**.

CRYPTOLOG
July 1994

by [   ]

P.L. 86-36

(U) The first coordinated public cellular mobile communication networks came into service in 1981. Since that time, cellular mobile use has grown to the point that there are now over 20 million subscribers to these networks throughout the world. Until recently, all of these networks used analog transmission technology to transmit users' communications. In the late 1992-early 1993 time frame, however a second generation of public cellular mobile networks emerged using digital technology and employing advanced multiplexing methods and modulations. These second-generation digital networks support a variety of new user services and provide for a number of improvements over existing analog cellular mobile networks.

(U) Two digital cellular mobile standards are presently being employed: the IS-54 digital AMPS (DAMPS) in the United States and the pan-European Global System for Mobile Communications (GSM) in Europe. Other standards are also being developed and may emerge in the not-too-distant future.

What is the Global System for Mobile Communications (GSM)?

(U) An oversimplified definition is that GSM is a **public telecommunications system.** The original expansion and eventual system name was derived from the initials of a Conference of European Posts and Telecommunications Administration (CEPT) working group Groupe Speciale Mobile (GSM). CEPT established the

public cellular mobile radio "standard" aimed at beginning public service in the early 1990's. Following the 1982 inception, two significant events occurred. First, in 1987 the original GSM system's specifications were modified to reflect a change in technology from analog to digital, due mainly to operational simulations and trials conducted in Paris under the supervision of the GSM working group. Then in 1989, the GSM program was transferred from the purview of the CEPT to the European Telecommunications Standards Institute (ETSI). Since that time GSM's official expansion has become "Global System for Mobile Communications," and ETSI continues to oversee the development of GSM.

(U) GSM is a public digital cellular mobile radio system intended to become the standard for the whole of Europe and differing greatly from the many cellular mobile systems currently in existence throughout Europe and the rest of the world today. It will offer connectivity to all public telecommunications systems, both national and international, and offer all the same services and compatibility of a fixed telephone, including Integrated Service Digital Networks (ISDN), without the restriction of wires.

Who developed GSM?

(U) Non-cellular mobile radio communications systems have been in use since the 1920's; however, public cellular mobile networks did not come into service until 1981. Papers describing the concept had been written decades before, but it was not until the 1970's, after the emergence of reliable microelectronic circuits, that practical cellular communications systems could be developed. By the late 1970's, the telecommunications administrations of the Nordic countries (Sweden, Denmark, Finland, and Norway) had developed the Nordic Mobile Telephone-450 Standard. In 1981, while the rest of Europe, the United States, and Japan continued their cellular research, the Nordic countries began public service with the NMT-450, a coordinated mobile cellular communications system that uses analog technology and operates in the 450MHz frequency range.

(U) By 1982, European telecommunication administrations interest in cellular communications was growing and the market was expanding rapidly. CEPT,

realizing the growth potential of public cellular communications and a need for standardization among these systems, established the GSM Working Group. Specifically, it was tasked to provide an outline definition by December 1986 and a specification for a Pan-European public land mobile network by December 1988. Early in 1983, the working group had identified all competing systems and proposals, none of which were acceptable as candidates for the Pan-European system. To avoid standardization obstacles and any interference with the development of a new, clearly defined Pan-European system, the working group declared that all existing systems and system proposals would be considered "interim" systems.

(U) In 1987 the Ministerial Council of the European Community (EC) urged all member countries to introduce the GSM system. According to this recommendation, the start date for the Pan-European digital cellular mobile radio system should be no later than 1991, the most important city areas should be covered no later than 1993, and the main connections between covered areas should be no later than 1995. This recommendation was adopted in 1987 through a memorandum of understanding (MoU) between operators and telecommunications administrators of 16 European nations. Since then, others have signed the MoU, bringing the total number of signatories to 23 operators in 16 European countries, as well as another 20 countries throughout the rest of the world. Most of these countries have agreed to abide by the terms of the EC recommendation including the stipulation to license at least two operators, one private and one public, thereby creating a competitive consumer market.

(U) As the GSM working group's activities progressed, it became quite apparent that the analog systems currently deployed in Europe were overburdened and would be unable to meet future demand for public mobile cellular communications. Therefore, in 1987, it modified the GSM system specifications, citing a change from analog to digital technology. Since 1989, when the program was transferred from CEPT to ETSI, work on the GSM standard has continued as planned, and CEPT continues to provide an open meeting place for European telecommunication standardization activities. It should also be noted that, although CEPT and ETSI have been the overseers of the GSM program, various ad-hoc subgroups and joint groups have been formed periodically to assist in the development of the GSM standards. At one time there were as many as 28 groups involved in the writing of the standard, as well as the theoretical, practical, and simulation studies associated with the program.

Why was GSM developed?

(U) Development of GSM is particularly important at this time, due to the political and economic changes sweeping the world today. Many of the Third World countries (including those in East Europe), are attempting to develop market economies patterned after those of the West, to which efficient communications are essential; therefore, many of these countries are planning massive upgrades of their telecommunications infrastructures and are intent on deploying state-of-the-art equipment in order to compete.

(U) Funding for such upgrades, if not nationally available, is in most instances readily available through various lending institutions like the International Monetary Fund and the European Bank for Reconstruction and Development, or through joint ventures with many western companies designing and building GSM-compatible equipments.

(U) Various factors have driven the development of the GSM system, but probably the most important of these was the need to develop a standard to be adhered to by all digital mobile communications equipment manufacturers and suppliers. This standard will insure compatibility between equipment and provide a capability for the user to roam freely throughout Europe while maintaining communications with another party, be it through speech or data.

(U) Another major factor was the phenomenal growth in the use and deployment of public analog cellular mobile networks. Several European countries, as early as 1983, had deployed mostly non-compatible systems operating in the 450MHz band. This rapid growth, especially in the Nordic countries, resulted in pressure to allow these systems to migrate operationally into the 900MHz band—a logical migration, since the International Telecommunication Union (ITU) had already obtained approval from the World Administrative Radio Conference (WARC) to have this band designated for public mobile communications use in Europe.

(U) The United Kingdom was the first to allocate a portion of the 900MHz band for the operation of their first-generation analog system, known as the Total Access Communications Systems (TACS). Since that time, other countries have followed suit, and the U.K. has gone one better by allocating more of the 900MHz band, just below the original GSM spectrum allocation, for the operation of its Extended Total Access Communications System (ETACS).

(U) The ETACS expansion illustrates just one of the perceived benefits of the GSM system, High Spectral Efficiency. As GSM is introduced, it will be facing fierce competition from numerous analog systems already operating in the majority of the 900MHz band. Therefore, it must use its limited spectrum allocation (905-915MHZ and 950-960MHz) more efficiently than current analog networks. This reportedly will be accomplished through the use of a more complex control system. It is envisioned that the GSM system will eventually migrate to occupy the whole 50MHz, of the 900MHz band designated for public cellular mobile communications throughout Europe (890-915MHz and 935-960MHz). Until this occurs, however, the digital GSM system must perform far better than any analog system within its limited spectrum allocation to be an attractive marketable alternative.

(U) Cost-efficiency is also another benefit of GSM deployment. Initially, equipment costs may be higher than that of present analog equipment for the subscriber as well as the network operator. However, as additional features are introduced by the network operator the GSM equipment actually becomes more cost-efficient for both the subscriber and network operator.

(U) To date, all operational GSM systems are in their infancy and provide no more than national telephony service. Additional services and capabilities such as international roaming and ISDN will be phased in as software is developed and tariff and billing arrangements are established among national operators.

(U) The network operators benefit because there is no additional equipment to purchase when introducing the new features, since they will have the digital equipment in place and the additional features will be incorporated through the introduction of software at a minimal cost. Subscribers will be provided with these additional services as the operator introduces them, probably at a minimum additional charge, and in the end enjoy all the benefits that an analog system cannot provide. Other advertised benefits are smaller, smarter, lower-cost terminals; digital speech quality; improved mobile data and facsimile transmissions; built-in encryption; integral short message capabilities; and the added dimension of national and international roaming.

(U) Overall, the digital GSM cellular system will provide the user with smaller equipment, better quality communications, and all the services normally available on a fixed public telephone network.

Future Use

(U) Estimates vary, depending on the source, but it has been projected that there may be as many as 20 million European subscribers to the Pan-European service by the turn of the century. Future deployments are projected for all western European countries and the central European countries of Cyprus, Hungary, Poland, Turkey, the Czech Republic, Slovakia, and Greece. A number of other countries are considering GSM technology as a basis for their future digital mobile communications network deployments. These include, in the Far East, China, Australia, South Korea, New Zealand, Thailand, China, and Singapore, and, in the Mideast, Bahrain, Kuwait, Oman, Qatar and the United Arab Emirates, just to name a few.

(U) Based on the above projections and the apparent head start the Europeans have on their competitors (the United States and Japan) one could easily see GSM becoming more than a European standard as the world's telecommunications systems migrate from analog to digital technology. It is highly unlikely, however, that the GSM standard will be universally accepted; more likely it will be considered the first step toward the development of a global digital cellular mobile standard.

(U) Many factors will influence the deployment decisions. In the EC, the desire or need of the government to participate in the European "one market" philosophy will be an important factor. Other countries must consider their economic situation, the availability of the required frequency spectrum, and any restrictions which might be imposed by a successor organization to the Coordinating Committee for Multilateral Export Controls (COCOM). Additional considerations include the current state of a country's telecommunications infrastructure, for example the existence of any analog cellular systems and their potential for growth as well as the availability of any competing digital standards.

(U) The acquisition of GSM systems will thus vary from country to country. Many will jump on the bandwagon right away; some will initially deploy analog cellular systems, while others may decide to play a waiting game (especially if they have an adequate telecommunication infrastructure), to see which digital cellular technology, if any, will be accepted as the global standard. The likely scenario for the European continent is that all the western European countries and some central European countries will, as stated above, deploy GSM systems as soon as possible, while the remainder will probably deploy analog cellular systems to augment their inferior telecommunication infrastructures. Even-

tually, even those countries who initially chose an analog deployment will probably migrate to the GSM standard.

(U) Adoption of the GSM standard by other world nations should also follow the pattern set by those countries throughout Europe. In the lesser-developed and Third World countries some will go the route of the western European countries and immediately deploy GSM systems, providing they can obtain the funds and COCOM-successor restrictions do not apply; others will delay deployment. In developed nations the need to immediately adopt a new cellular mobile standard will be less critical, since most have well-established telecommunication infrastructures to include a number of operational analog systems, or are in the process of developing their own digital cellular mobile standard, as is the case with Japan and the United States.

(U) Therefore, the world's cellular mobile telecommunications picture will most likely, at least in the near term, remain a hodgepodge of analog and GMS digital cellular mobile communications systems, and the number of users/subscribers switching to the new GMS systems will not increase dramatically, due to the initial high costs of equipment and subscribership. In the long term however, as more services become available and costs decline, GSM will undoubtedly become a viable option for the public sector.

Conclusions and Recommendations

(U) **GSM systems provide highly sophisticated communications.** The vast majority of cellular systems currently deployed throughout the world today are incompatible analog systems providing, at best, a national voice telephony capability and other limited services. When these systems are compared with a mature GSM digital system it becomes quite evident that the additional capabilities of GSM—increased data rates, improved signal quality, improved spectrum usage, improved security of communications, and compatibility of systems among countries—provide a cellular mobile communication system far superior and more sophisticated than those in use today.

(U) **GSM system deployments and subscribership will increase.** There will be a continual migration from analog to digital mobile cellular communications, and the number of system deployments, as well as the number of subscribers, will increase as new phases of the GSM standard are introduced, additional services become available, and the costs of equipment and sub-

scribership to GSM networks diminish. The rate at which this migration and growth of subscribership occurs will differ worldwide, because of variances in governmental telecommunication policies, the current state of an individual country's telecommunications infrastructure, a desire to perpetuate a global market, subscribership growth potential of current analog mobile cellular communications systems, availability of the required frequency spectrum, and the development of other digital cellular standards possibly providing capabilities superior to the GSM standard.

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

by
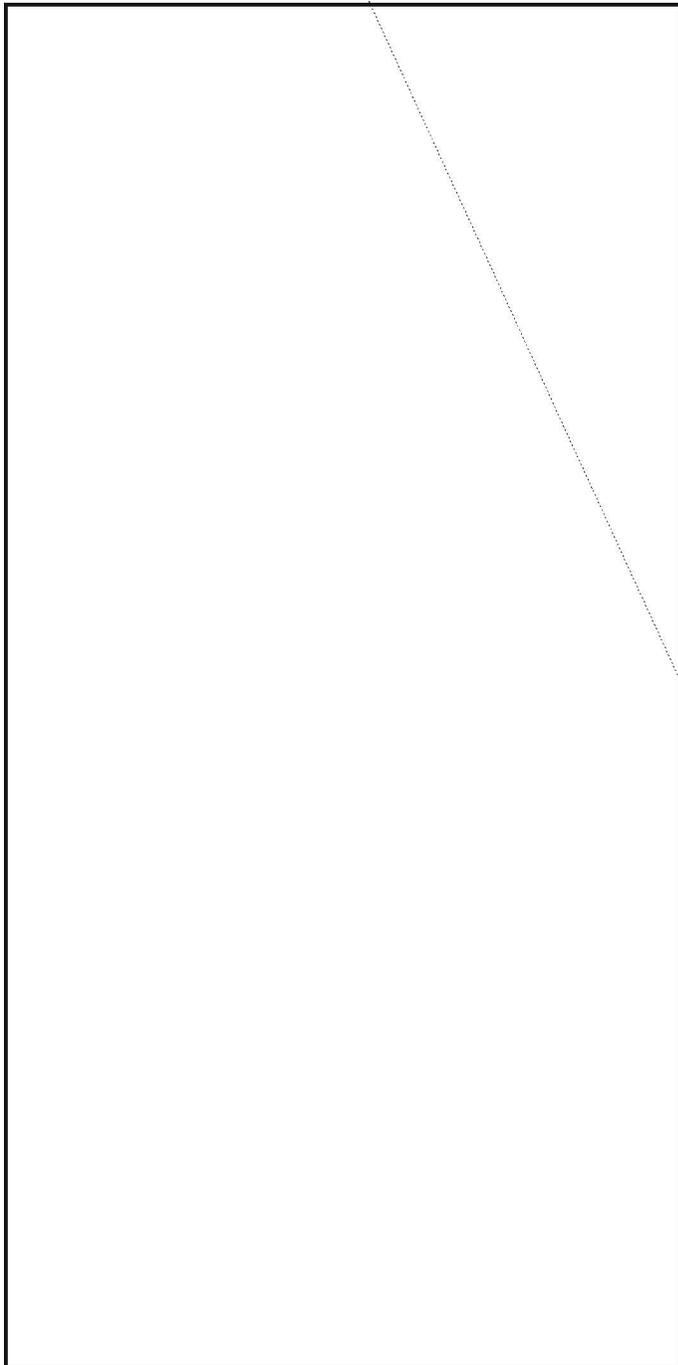
P.L. 86-36

(U) In the past several years, there has been a virtual explosion in the use of digital means for transmitting voice telephony and other services. The most prevalent method of converting analog information to digital pulses is pulse code modulation (PCM). Many countries have already made, or are in the process of making, substantial investments in the installation of PCM systems. Third World countries in particular have been rapidly expanding into the digital arena while Western countries are doing so at a slower rate, chiefly because the lack of existing communications infrastructures in the Third World makes a direct move into digital systems economical.

(C) Western countries, on the other hand, have invested significant resources in their analog systems, and therefore tend to replace existing systems at a slower pace. The growth rate in digital transmissions in the West over the next several years is anticipated to be about one to two percent per year. This pace is significant enough that it cannot be overlooked by the Intelligence Community.

(U) Economic considerations, enhanced signal quality, and the inherent flexibility of the digital transmission network are important factors in the shift from analog to digital transmission. In addition, many vendors are no longer producing analog FDM systems, thus forcing users to replace them with digital systems. Fiber-optic cable is the preferred mode; however, terrestrial microwave is expected to remain prevalent for short-haul transmissions and as a back-up to fiber.

(U) The concepts underlying PCM have been understood since the mid-1930s. France filed a patent in 1938; British and American patents were filed in 1939 and 1942 respectively. By 1948, studies in Bell Telephone Laboratories had proved that PCM was well understood. Because frequency-division multiplexing (FDM) was easier to implement and further developed than time-division multiplexing (TDM, the basis for PCM), however, FDM was virtually the only transmission mode then in use. The advent of the transistor in the late 1950s helped solve the problems surrounding the implementation of PCM, and American Telephone and Telegraph introduced PCM in the early 1960s.

(U) There are two primary PCM hierarchies in use throughout the world: the CEPT (Conference of European Postal and Telecommunications) or European standard and the North American/Bell standard. The Japanese have developed their own standard, based on the Bell system; to date it has been seen in use only in Japan. Each standard operates on a building-block principle. Voice-grade channels are multiplexed in the basic level to form channel bank units (CBUs), also referred to as the Level 1 multiplexer. Level 1s are combined to form successive signal levels and increasingly higher-capacity systems.

CEPT Standard

(C) CEPT, the European standard, has been accepted by the International Telegraph and Telephone Consultative Committee (CCITT) as a standard in the international PCM arena. In this system, each frame is made up of a set of 32 channel time slots numbered from 0 to 31. Voice channels are allocated to 30 channel time slots. Time slot 0 is reserved for frame alignment and alarm indication facilities and 16 is used exclusively for signalling; voice-grade-channel signalling is carried on this one channel rather than within individual channels as is the case with CCITT #5. This type of signalling is referred to as common-channel signalling (CCITT #6). Each channel time slot is composed of 8-digit time slots and sampled at a rate of 8000 samples per second; the complete frame repeats every 125 microseconds. The CEPT format produces a 256-bit frame (32 channels X 8 bits per channel) and an operating bit rate of 2.048 Mbps (8000 samples per second X 256 bits) employing A-Law companding. Level 1 (L1) signals are composed of 30 channels; Level 2, four L1s (120 channels); Level 3, four L2s (480 channels), Level 4 of four L3s (1920 channels), and so on.

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

EO 1.4.(c)

P.L. 86-36
EO 1.4.(c)
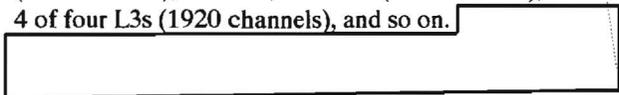
Bell/North American Standard

(U) The Bell/North American standard has also been approved by the CCITT as a PCM standard. The T1 carrier, also referred to as a Bell Level 1, was introduced by Bell in 1962 and allowed for the multiplexing of 24 voice channels over one transmission medium. Each voice channel is composed of eight bits, giving a frame length of 192 bits (24 X 8). A 193rd bit is used for framing and signalling control. The T1 operates at a bit rate of 1.544 Mbps (8000 samples per second X 193 bits). The T2, or second-level Bell system, was introduced in 1972 and carries 96 voice channels on a single transmission medium. The T2 is composed of four T1s, the T3 of seven T2s for a total of 672 channels and the T4 of six T3s for a total of 4032 channels.
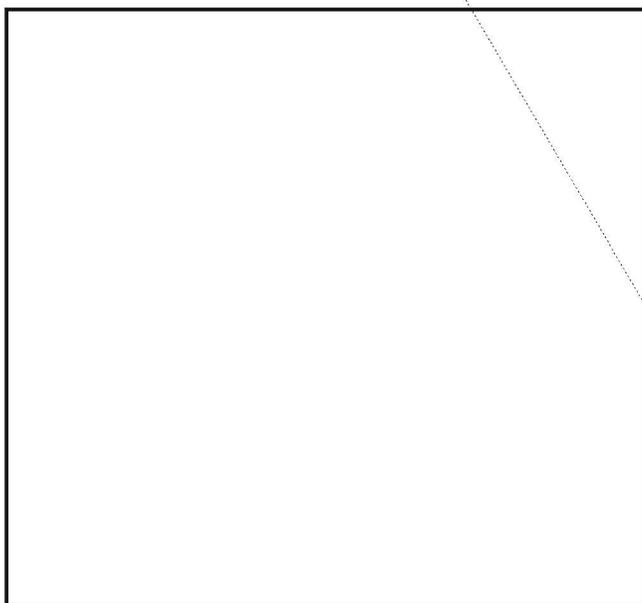
Advantages and Disadvantages of PCM

(U) PCM has several advantages over FDM analog systems. One of the primary advantages is its low cost. Unlike FDM systems which require many precise and elaborate band-pass filters throughout the system, PCM systems require only simple channel low-pass filters. Because of the decreasing costs of large-scale integration (LSI) technology, which is employed in the design and fabrication of PCM system electronic components, and the elimination of expensive filtering, the per-channel costs of PCM are much lower than those of FDM.

(U) A second advantage of PCM is its excellent speech quality and its improved signal-to-noise ratio (SNR) as compared with FDM transmissions. In analog transmission, disturbances caused by noise, cross-talk, intermodulation, and other factors cannot be eliminated

once introduced into the signal. Each time the signal is amplified, any associated noise is amplified as well. This is one of the most serious limitations of analog transmission systems. The PCM signal, on the other hand, exists in only two states: 1 and 0 (pulse or no pulse); as long as the presence or absence of a state can be detected, no matter how distorted the signal, the PCM system can handle it. The degradation of the received signal does not alter the information content until it becomes so severe that the receiving equipment cannot distinguish between the presence or absence of a pulse. In contrast with FDM, which is amplified at each repeater, PCM signals are regenerated at each repeater and are therefore not limited by accumulated degradation. Regeneration completely eliminates the perturbations of the preceding transmission, which means there is no limit to the transmission distance. This is one of the unique advantages of digital over analog transmission systems.

(U) PCM is very flexible, lending itself to all types of modulation schemes. Systems of different rates and carrying different types of service—telephony, data and other digital services—can be easily interconnected. Because it offers direct digital interface, there is no need for modems to convert digital signals to analog prior to transmission over a voice-grade channel. A channel capacity of 64 kilobits per second (Kbps) can be achieved with PCM as compared to a maximum of 2.4 Kbps on unconditioned FDM channels.

(U) PCM also has disadvantages. First, it requires approximately 16 times more bandwidth than FDM. In addition, in order to maintain transmission integrity, the signal must be regenerated frequently, approximately every 6000 feet on cable and at each repeater on microwave. Lastly, complex demodulation and demultiplexing equipment is needed for voice-grade-channel analog-to-digital conversion at the transmitter and digital-to-analog conversion at the receiver.

Conclusions and Recommendations

(S-CCO) It is clear that the worldwide communications environment is undergoing a transition from analog to digital. Cable appears to be the transmission means of choice; however, microwave will continue to be used for short-haul transmissions, in urban environments and as a back-up to fiber, thus making terrestrial microwave collection a viable mission. We can also expect to see increasingly higher data rates in use. Data rates of 140 Mbps are no longer unusual and it is anticipated that data rates up to 300 Mbps will become increasingly common over the next several years. In

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

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

CRYPTOLOG
July   1994

addition, new formats, such as forward error correction (FEC), trellis coded modulation, synchronous optical network (SONET), and synchronous digital hierarchy (SDH) will become more prevalent. Higher modulation levels such as 256 QAM can also be expected, as can increased military use of digital transmissions.
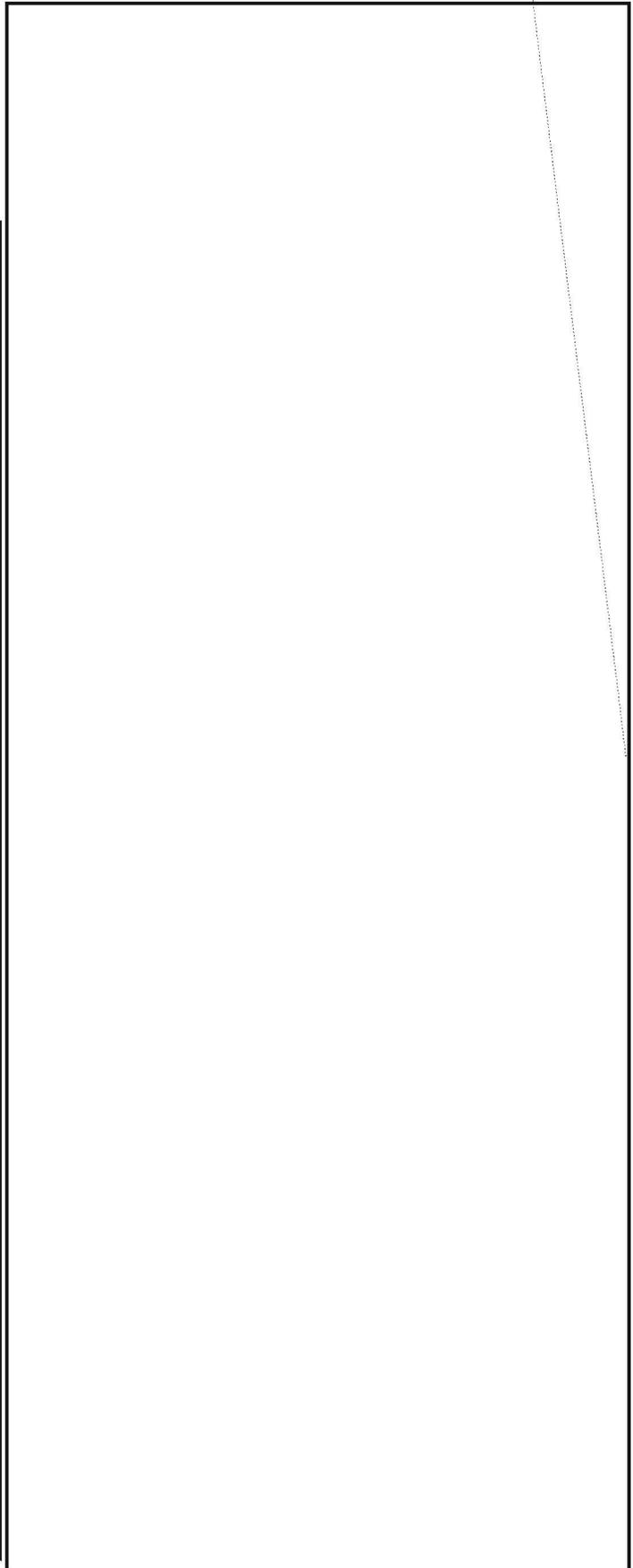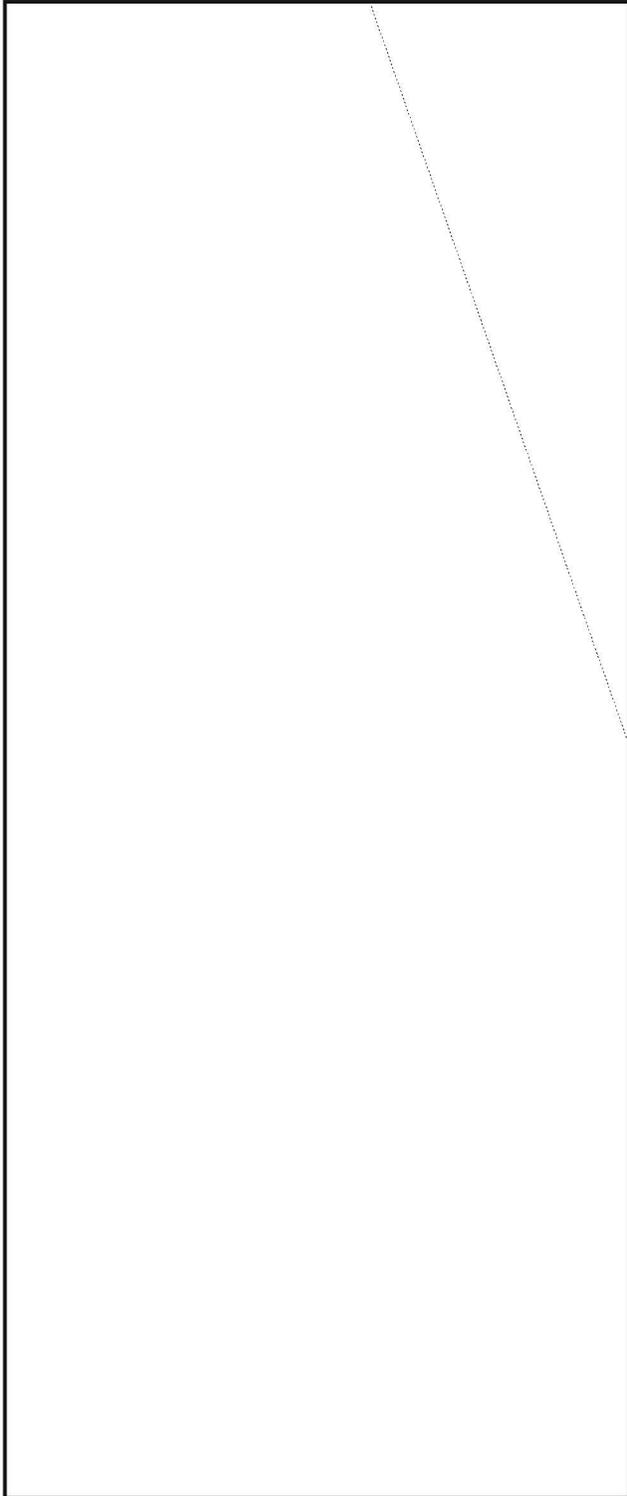
Video SIGINT Dissemination:

The NSA Broadcast Network

P.L. 86-36

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

by [ ] P0542

(C-CCO) SIGINT reactions to [ ]

These are the kinds of things you may see on television in the workplace, as the NSA Broadcast Center pursues its goal of bringing you the latest intelligence news from around the world, 24 hours a day.

(C) The NSA Broadcast Center has been broadcasting SIGINT for more than two years via the NSA Broadcast Network and the Defense Intelligence Agency's Defense Intelligence Network (DIN). Through the DIN, video SIGINT reports reach DIA, the Pentagon, numerous military commands worldwide, and certain Washington, D.C. users. Within NSA, classified broadcasts produced by the Broadcast Center appear daily on NEWSMAGAZINE Channel 21. Video SIGINT is a fast-growing medium, providing the busy executive, field commander, and target analyst with instant access to the world's daily headlines and breaking stories, in a readily absorbed form.

(C) Since July 1993, the Broadcast Center has been producing live programming that integrates live SIGINT updates, live and taped interviews, interviews remoted from organizations such as DEFSMAC, and taped special programs. All SIGINT Headlines programs are broadcast live to ensure they contain the most up-to-date information. In addition, the Broadcast Center's partnership with NSOC ensures that CRITICs of national level importance can be broadcast as soon as the information has been verified—meaning viewers will be able to learn of them faster than ever before.

How The Broadcast Network Works

(FOUO) Time-sensitive video SIGINT is a unique medium, yet it resembles commercial television news in many ways. Video SIGINT reporters aim for timeliness, while striving to meet the standards of commercial news presentations. Video SIGINT reporters—most with SIGINT reporting experience, a few from other SIGINT disciplines—work rotating shifts to cover the SIGINT news around the clock. All underwent a selection process involving a screen test and writing sample.

(C-CCO) A video reporter's day is probably at least as busy as that of a CNN correspondent. Arriving in the newsroom, he or she "hits the ground running," poring over the most recent SIGINT product (everything that enters [ ] is distributed electronically to the Broadcast Center), selecting items based on their newsworthiness. First priority goes to items related to the hottest news stories of the day. In addition, reporters focus on product related to regions of current policy-maker interest as listed by the White House Situation Room, or product deemed by the executive producer to be of intelligence interest. Using the selected product, reporters write video scripts, design graphics, and select appropriate video footage. Meanwhile, skilled computer graphics artists convert the reporters' rough sketches into professional on-screen graphics that can incorporate maps, photographs and footage stills.

P.L. 86-36

(U) After the scripts have been edited and approved by the executive producer, the reporter becomes an on-camera anchor, seated under bright lights in the Broadcast Network's studio, reading scripts as they scroll by on a teleprompter. Next, words meet pictures in the Broadcast Network's control room, where video editors, many with commercial television experience, combine the live or taped narration with graphics and footage. In spare time, the newsroom crew carry out innumerable logging and housekeeping duties. In even sparer time, they put together long-term video background reports. In addition, both reporters and executive producers conduct on-camera interviews.

(FOUO) Executive producers, the shift team chiefs, perform all the functions of a reporter. In addition, they are responsible for content and quality control of all programs written and produced on their shift. After normal duty hours, the executive producer has Senior Reporting Officer-equivalent authority as the last

person to see NSA visual product before it is released to the DIN and its audience. On days, the producers also do program planning, work on developmental program projects, coordinate the Broadcast Network's activities with Intelligence Community customers, and brief visitors on the Broadcast Network's operations.

NSA Video Compared With Commercial Television

(C) Just as commercial television news is faster than print media, video broadcasts have the potential to get the SIGINT fact to the customer faster than standard database pulls, whether on a computer screen or in a stack of paper. At the same time, video aids the viewer through use of graphics such as maps, bulletin boards, photographs, and footage clips. Interviews, a staple of commercial television news, are also proving highly effective in providing SIGINT target expert knowledge and background that are not generally included in SIGINT product.

(C-CCO) Video SIGINT differs from commercial television, however, because SIGINT stories respond to National SIGINT Requirements and thus lack the sizeable entertainment component (such as stories broadcast strictly for their humorous, bizarre, or human interest content) of commercial news. Another factor that makes video SIGINT "look" different is USSID 18, which by forbidding the intercept of U.S. communications, results in a distinct lack of local news!

Video Complements Written SIGINT

(C) While television news serves a different purpose than print-media news, it definitely has not replaced it, and so it will be with video SIGINT. In the commercial world, print news media have largely ceded the breaking-news aspect of journalism to electronic broadcast media. In somewhat the same way, televised SIGINT will ultimately serve the person who wants the latest news now, at the push of a button, without having to touch a piece of paper or even read a screen. SIGINT on television will also serve the busy executive or policy-maker with little time or inclination to read, as well as the busy analyst with a yen to know what's happening in SIGINT around the world. When large numbers of customers gain access to video terminals, time-sensitive video is potentially the most efficient way to get the basic facts to the most people.

(C) Video SIGINT's role is to parallel, complement, and enhance SIGINT in written form. Time-sensitive written-media SIGINT product will, of course, continue to convey vital intelligence to users. For many

purposes, including decision-making, people require written reports they can mull over, carry to the next office and discuss, and have sent to them via electronic mail.

(FOUO) Television won't replace longer-term SIGINT product, or SIGINT summaries, either. Consider that commercial television has been available for nearly 40 years. While there are far fewer newspapers now than there were 40 years ago, most people still peruse at least one daily paper for in-depth background and analysis of the day's events. As electronic journalism has taken over delivering breaking news, print media have expanded their capacity to give "the full story," to provide perspective, and to serve as the media of record. It is unlikely that a well-informed person, such as an NSA employee, would consider television news sufficient to keep him or her up to date. To an even greater degree, the same considerations apply to SIGINT and other intelligence delivered by video or in written form.

(C) However, video SIGINT possesses a unique extra dimension not possible in written form: television interviews. While all SIGINT reporting answers the question, "What did NSA intercept?" interviews can answer, much faster than the written word, the important question, "What does NSA think?" Policy-makers and other customers want and need the benefits of NSA's immense reserves of analytic expertise. To stay informed and make decisions, they require access to the intuition and experience of SIGINT analysts, who in many cases have studied their targets for decades. In a five-minute television interview, an expert analyst can give large numbers of viewers a great deal of valuable knowledge about the "hot" topic of the hour. To this end, NSA's SIGINT Intelligence Officers (SINIOs) are interviewed regularly on the Broadcast Network.

Other Applications For Video SIGINT

(S-CCO) Television, in addition to its unique time-sensitive uses, has many applications for long-term SIGINT analysis and background. A short video feature can untangle complex facts about a SIGINT target. Broadcast Center reporters have produced video term studies

EO 1.4.(c)
P.L. 86-36
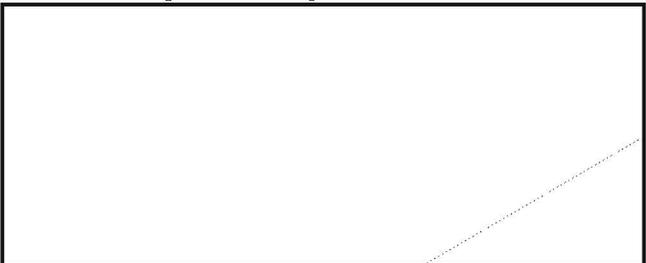
(C) The possibilities for fusing SIGINT with other intelligence sources, such as human intelligence, imagery, and open source news, are unlimited. During a crisis, video features, combined with expert analyst interviews, would give policy-makers a snap course in events leading to, say, a coup in a foreign government. Customers would learn factors affecting economic relations between the U.S. and another country, or discover key people who may affect the outcome of elections in a fragile new democracy.

(C) Besides disseminating SIGINT, video term reports can benefit a diverse audience by addressing collection, management, and personnel issues. Such reports would benefit the viewer by rounding out the picture of what NSA does, NSA's role in the Intelligence Community, and how the individual fits into the intelligence picture.

Audio SIGINT News Service

(FOUO) No NEWSMAGAZINE terminal yet, and no word on when your office will get one? You can still hear the latest SIGINT news through the Broadcast Center's Audio News Service by dialing 963-NEWS. It is updated, 24 hours a day, with each edition of the SIGINT Headlines and Highlights; plans are to include other SIGINT news programs as well. During weather emergencies, when the DIN closes and the Broadcast Center does not retain enough personnel to do video programming, the Headlines will continue to be updated daily.

Much Work Yet To Be Done

(FOUO) Although video broadcasting at NSA is constantly expanding, there is a long way to go before video is delivering all the "SIGINT on the spot" to every customer who needs it, at NSA, in the Intelligence Community, and within military commands. Some issues that must first be addressed include:

• Increasing the number of NEWSMAGAZINE terminals (presently there are about 400) throughout NSA. Access currently is limited by the number of terminals, as well as by security and distribution considerations. Our broadcasts may not use compartmented product, and certain ORCON Intelligence Source Indicators are off limits as well.

• Expanding the NSA Broadcast Network to include National Cryptologic Representatives, Cryptologic Support Groups, Special U.S. Liaison Officers, and ultimately, field sites and Regional SIGINT Operation Centers.

• Establishing remote video links for two-way broadcasts.

• Expanding our partnership with NSOC.

• Increasing the Broadcast Center's manning, resources, and space, and going on line 24 hours a day, 7 days a week.

• Tailoring our programing to a variety of customers downtown and around the world as the DIN expands its customer base.

Thanks to the Tech Trend Notes, which publishes a Calendar of Events sponsored by NSA, academia, and professional associations, there is now a greater than ever opportunity to disseminate information on technical breakthroughs to the workforce. Here's a sample of what's happening this year:

Event	Date	Location	Where to call:
DoD Database Colloquium '94	29-31 Aug.	San Diego, CA	(703) 631-9125
Satellite Communication Users Conference	19-21 Sep.	Oak Brook, IL	(312) 938-3500
INFOTECH '94 Conference & Exhibition	11-13 Oct.	Dayton, OH	(703) 631-6200
Global Telecommunications Conference	27 Nov.-1 Dec.	San Francisco, CA	(415) 375-4338

SIGINT Glossary

Communications Analysis Trivia:

The GUHOR Stick

P.L. 86-36

by [ ] P0542

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

This is the first of what we hope will become a regular feature. Contributions from the Agency's corporate memory are welcomed.

(U) The what? No, it's not a Russian popsicle or the latest dance craze in Bosnia. It's only the most important tool ever invented for the traffic analyst of yore. Solutions to the most intricate communications networks often began with this simple device. No self-respecting TA was ever without one close at hand. Like the six-shooter of the old West, the analyst kept it at his side, always ready to draw—circles, boxes, and lines, that is.
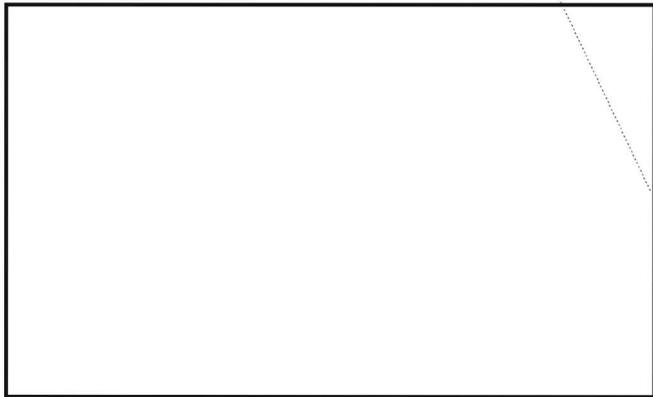
(U) The GUHOR Stick, in its most recent and best-known iteration, is merely a 6" by 1.5" clear plastic template. Its prime purpose is to facilitate the drawing of communications diagrams, although its secondary uses are endless. It comes equipped with a large circle at one end to draw control terminals, a smaller circle at the other end for outstations, and a small rectangle in the center for communications relays and CQ calls. The straight edges are used to connect these stations and show communications paths. With this tool, a #2 pencil (with extra erasers), some graph paper, and several pencils of various colored leads, the analyst of old was fully prepared to face any communications adversary.
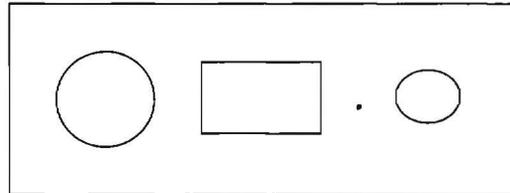
(U) But whence came this strange name? A GUHOR Stick? Putting my analytical skills to work, I set out to research the issue. To my surprise, there was a higher than expected number of individuals who had heard the name. Most were seasoned veterans from a mixture of professions, including linguists, reporters, managers, executives, and, naturally, traffic analysts. But there was more than a little discussion about what this device was and where its name originated.

(U) The early returns were mixed, however. I was still searching for the definitive word. It was at this point when I began to get responses via e-mail from

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

1. Those on field duty in the Pacific used a similar device which they called a "pooka-maker." Pooka is a Hawaiian word for "hole."

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

members of a Communications Analysis Association (CAA) interest group. A number of seasoned veterans recounted their GUHOR experiences and, in a number of colorful responses, gave me what I believe to be the true scoop.
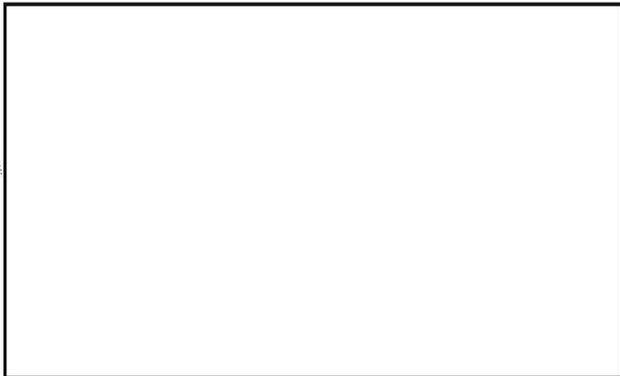
(U) GUHOR Sticks as traffic analysis tools have been around for decades. Some CAA respondents remembered seeing or using them in one form or another from at least the early 1960s. Even so, a couple of questions remain unanswered. Who invented it? Why was it given this curious name? Someone out there knows. If you can solve the mystery, we're ready to hear a good story.

(U) All this discussion about GUHOR Sticks may be moot. These devices are few and far between these days. The GUHOR Stick does not have a federal stock number. They were made in batches at NSA by special order; however, they are fast becoming collector items. With the advent of the desktop computer, many analysts are using computer graphics to diagram their targets. The traditional circles and lines on paper are becoming passe. Most GUHOR Sticks that are found are being employed for many a sundry task—not for crafting the intricate networks of old, but for drawing nondescript lines and symbols unrelated to the trade of traffic analysis.

(U) Now, is there a similar wealth of knowledge out there about the Chun Wheel?

The author would like to thank the many CAA members whose phone calls and e-mail postings contributed to this article.

CRYPTOLOG

Editorial Policy:

(U) Technical articles are preferred over non-technical; classified over unclassified, shorter over longer., Emphasis should be on improving NSA's technical performance; articlesshould be aimed at explaining one's discipline to those outside it. Readers are also invited to contribute conference reports and reviews of books, articles, software, and hardware that pertain to our missions or to any of our disciplines. Humor is welcome, too. Submissions may be published anonymously, but the identity of the author must be known to the editor.

Submitting Items

N.B. If the following instructions are a mystery to you and your local ADP support is no help, please feel free to call the CRYPTOLOG editor on 963-3123s.

(FOUO) Send a hard copy accompanied by a labelled diskette to the editor at P054 in 2E062, Ops. 1, or For maximum efficiency (as far as possible within the limits of your word processor):

P.L. 86-36

- Do not type your article in capital letters.
- Classify all paragraphs.
- Label all diskettes, identifying hardware (OS: DOS, UNIX), density and type of word processor used.
- Put your name, organization, building and phone number on diskettes.
- FrameMaker format is preferred; ASCII is also fine. J334 has a conversion service that converts Interleaf, Word Perfect, OfficeWriter and MS Word into FrameMaker. Just attach the document to an E-Mail Compose Window addressed to **convert@po**.