DOCID: 4019609

~~TOP SECRET~~

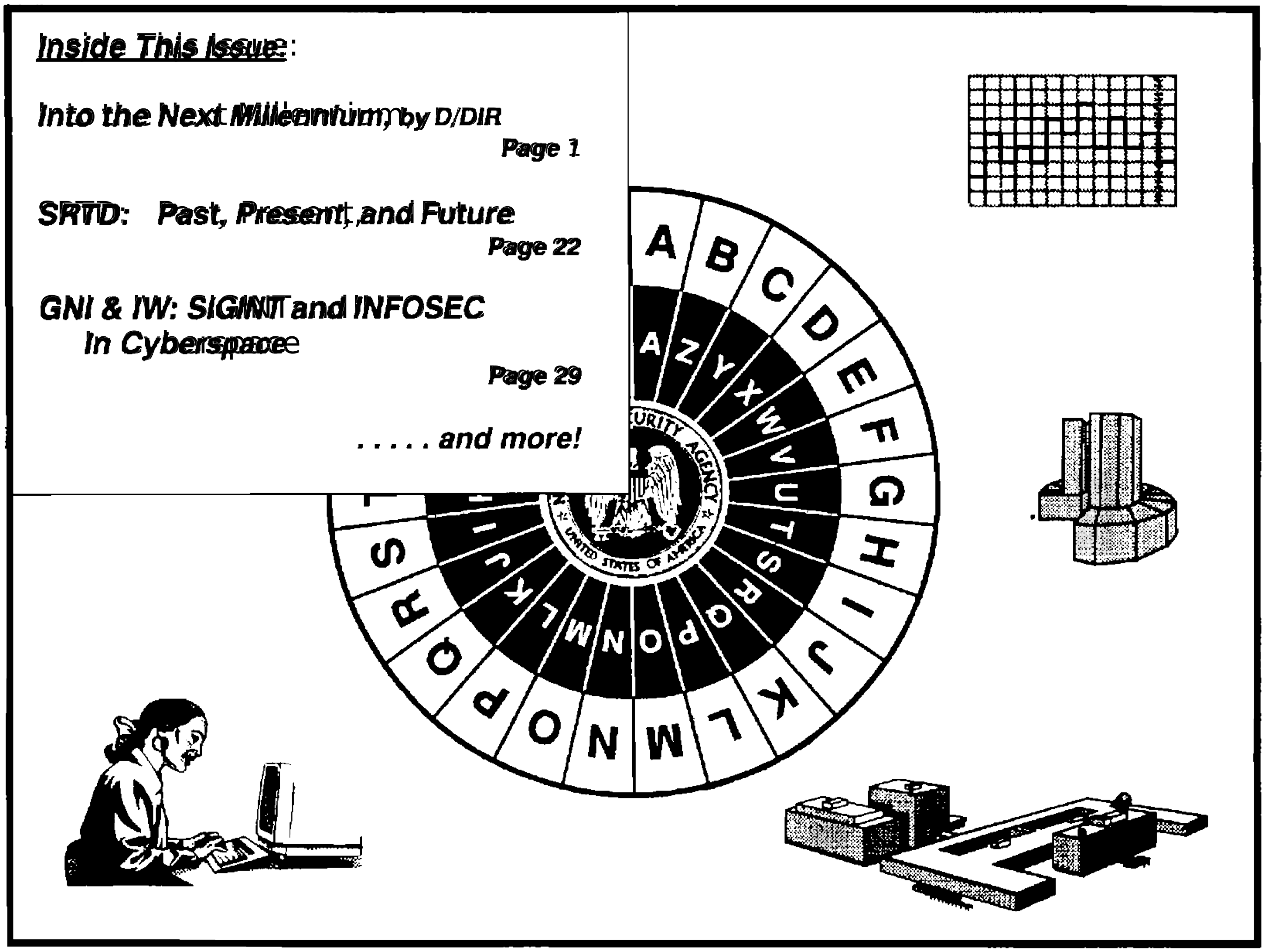
NATIONAL SECURITY AGENCY

CRYPTOLOG

The Journal of Technical Health

1995

VOL. XXI NO. 1



Inside This Issue:

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating Agency's Determination Required~~

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

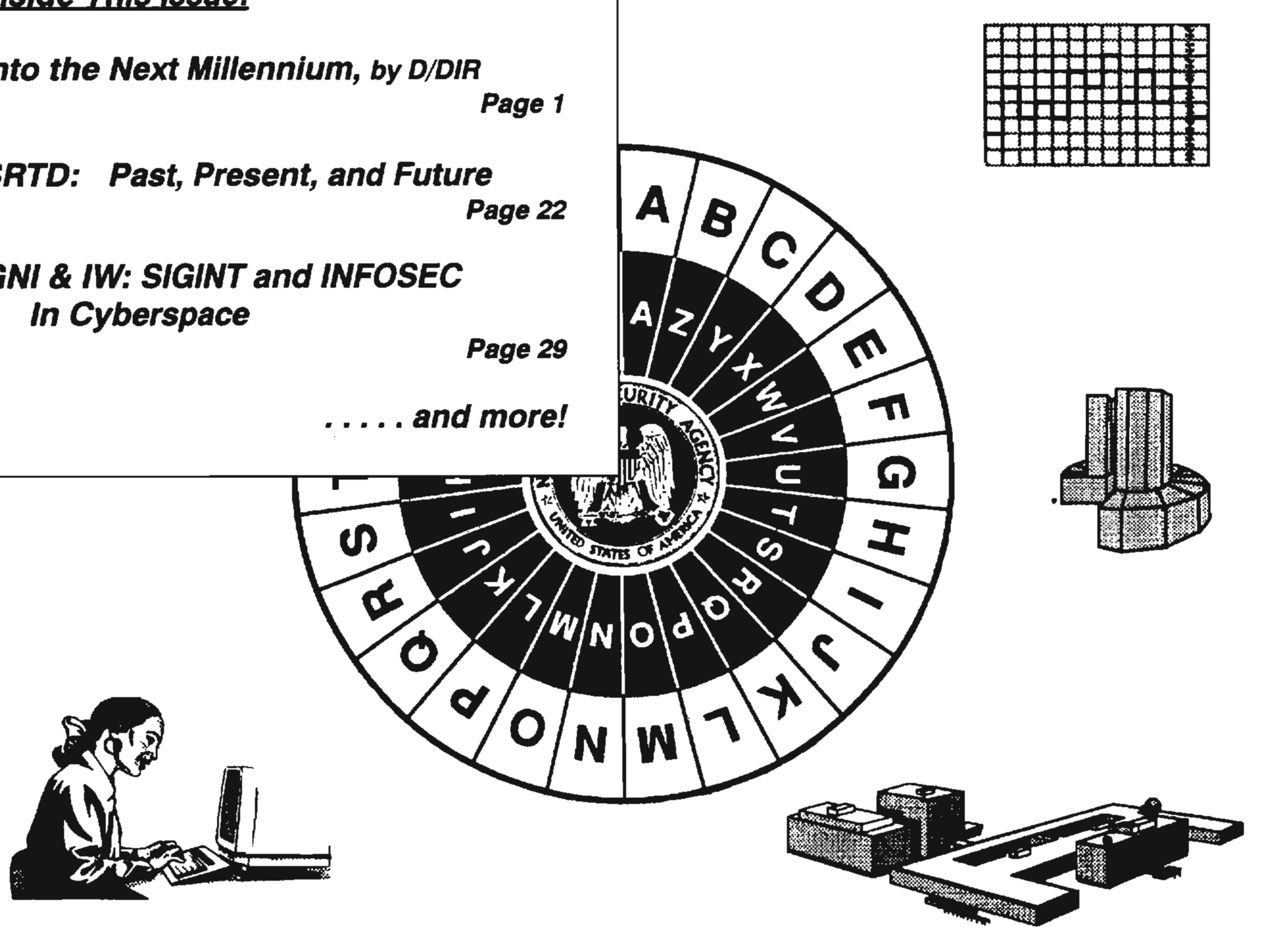
NATIONAL SECURITY AGENCY

CRYPTOLOG

The Journal of Technical Health
1995

VOL. XXI NO. 1

Inside This Issue:



CRYPTOLOG

Vol. XXI / No. 1

Published by P05, Operations Directorate Intelligence Staff

Publisher .... William Nolte (963-3123)

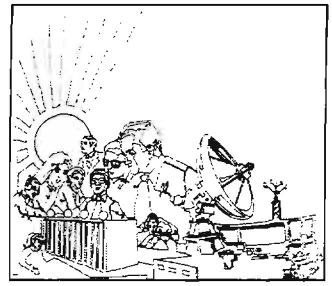
Editor .... [redacted] (963-3123)

Board of Advisors

To submit articles and letters, please see last page

CRYPTOLOG
Issue 1 1995

Table of Contents



CRYPTOLOG
Issue 1 1995

Welcome

On behalf of the chairman and members of Board of Advisors, welcome to this very special issue of *Cryptolog*. For over twenty years, long before the phrase "technical health" came into fashion, *Cryptolog* has promoted excellence and dialogue among NSA's professional work force.

Within that tradition, and at a time when the Agency and the Intelligence Community are facing fundamental review and revision, it is appropriate that *Cryptolog* should sponsor a survey of the cryptologic disciplines. We are appreciative of the work of the career panels whose fields are represented here for their assistance in the planning and preparation of this issue. We are especially honored to have the Deputy Director, Mr. William Crowell, as our keynote author.

In presenting itself to the various external groups studying the future of American intelligence, as well as in its own internal studies, NSA has consistently held to a fundamental principle: that cryptology is a process dependent on success across a range of individual skills and capabilities. It is the integration of those skills and our ability to communicate across disciplinary lines that has allowed that process to perform successfully over the last forty years. Our success in the next century will require no less.

Cryptolog has a new look, a new and active advisory board, and a renewed mission. Ultimately, however, its success depends upon the willingness of NSA's talented, multidisciplinary work force to continue and advance the dialogue of techincial health and technical excellence. We invite your participation.

Information Technology: Into the Next Millennium

by William P. Crowell, Deputy Director

(U) Not long ago while driving to work I saw a bumper sticker that really caught my eye. It said: "The Universe is Subject to Change at Any Time. . . And It's Right on Schedule."

~~(FOUO)~~ I think this really describes the universe in which we are living and will experience right into the next millennium. Most of us expect to see continuing rapid changes in technology, but with this rapid technology change come many other social and organizational changes as well. We can expect:

- Increasing pressures for organizations to respond to technology by decreasing cycle times for new products and new services;

- Increasing challenges to the Government's monopoly in areas of specialized information services, e.g. information on economic performance, personal information, and related services . . . AND intelligence . . . AND information-security services.

- Increasing opportunities for us to use technology to allow us to cope with these challenges and pressures, e.g., the use of information technologies and communications connectivity to achieve increased teamwork and knowledge-sharing.

~~(FOUO)~~ The key question for NSA is whether we will take advantage of new technology to help us advance our mission, or will we instead be whipsawed by new technology, be slow to respond, and merely be reactive to new developments that affect our business?

~~(FOUO)~~ In a 1978 CRYPTOLOG article, I argued that we were moving too slowly in responding to the opportunities posed by personal computers that were just then coming into widespread use. In my mind, PCs represented a potential major improvement to the SIGINT analysis process that would allow NSA analysts to move beyond the paper-and-pencil approach we had been using for 30 years. However, our computer acquisition efforts in 1978 focused on buying more of the large-scale computers we had bought in previous years. While these machines were necessary, it seemed to me that we needed to invest as well in small computers that would support analysts more directly and give them personal contact with their data. My observation at the time was: "This is one case where the bureaucratic process has developed a life cycle that far exceeds the cycle of development of new systems and capabilities and costs outside NSA."

~~(FOUO)~~ Where are we now? Well, I think everyone would agree that we have done a lot to improve the technology supporting our analysts. At the same time, technology has continued to advance, our budget has declined, and the world has changed dramatically. The real changes in technology—size, speed, connectivity, together with declining cost—are having a profound effect on NSA's overall mission. In many respects, we find ourselves now, in SIGINT as well as in INFOSEC, in a situation I would describe as hanging on by our fingernails. We're making good progress in many areas, but as the technology explosion continues, we need to move faster to keep pace. In terms of keeping ahead of the technology curve we're not much better off than we were in 1978.

~~(FOUO)~~ A quick review of breakthrough technologies that will affect our targets and our business between now and 2000 provides a sobering view of the challenges ahead. The sheer numbers of people with computers will drive increasingly rapid technology change. Quick and cheap access to information technology will mean that more of our targets will be converting to computer-to-computer communications. This is in addition to the use of facsimile, e-mail, and voice mail, all of which are already widespread. Multimedia will become a real challenge. The vision of the telecommunications industry—to enable people anywhere, anytime to exchange information simply, reliably, cheaply, and securely over their medium of choice—represents a true challenge to SIGINT in the future.

~~(FOUO)~~ The most startling changes, however, will be in size, speed, connectivity, storage technology, and cost. Size will drive the continuing development of personal computing devices: laptops, personal data assistants, and smart appliances such as digital recorders. Communications and connectivity (networking) improvements will make these devices more acceptable for real work. We will see more telecommuting, greater use of Mosaic-like browser capabilities on the Internet, and a much more complex set of technologies in use by target military forces. Increases in processing speed will allow for continuing performance improvements. Graphics interfaces will be more responsive, and today's relatively poorly-performing algorithms, such as those used for speech recognition, will be greatly improved. Storage technology injects an interesting uncertainty into technology projections for the future. It's very clear that the industry will achieve tens to hundreds of gigabytes at very low cost in the next 5 years. It is not exactly clear how these technologies will fit into the overall architecture of an increasingly networked world. (I can think of several NSA applications, however!) Finally, decreasing costs will fuel the whole cycle of change, promoting ever greater speed of change as the favorable economics of using new technology will push old technology out of the way.

~~(FOUO)~~ I believe the impact of these changes on NSA can be categorized in four interrelated areas:

➢ *Accumulation and availability of information.* This is the problem of data overload. There is much more information available now than ever before. We need to continue to improve our methods of accessing and storing this information in ways that are easily manageable and analyst-friendly. This also means that we may have to discard some of our traditional methods of storing data in the interests of improving efficiency and laying the groundwork for more rapid advances. We may also have to abandon some of our traditional approaches to collecting data, since it does not make sense to continue to collect data we don't or cannot use.

➢ *Organization and structure of work.* New demands for functional and horizontal relationships place strains on NSA's traditional organizational structure. I am not advocating another reorganization. I am saying that we need to build in much more flexibility into the way we approach things. The old boundaries between SIGINT and INFOSEC, between communications as a target and communications as part of our infrastructure, and between cryptologic disciplines, are rapidly disappearing.

➢ *Facilitation of teamwork in developing new skills.* We all know how successful NSA is in responding to crises. Bureaucratic walls collapse, procedural obstacles evaporate, and people pull together to provide unequaled support to policymakers and military commanders. We need to institutionalize this kind of teamwork during non-crisis periods, too. More than that, we need to encourage more cross-training among cryptologic disciplines. We need to provide mathematicians and intelligence analysts training in telecommunications and networking, for example, and we need to develop multi-disciplined signals collection officers who understand modern networks as well as the more traditional forms of communications still employed by some of our targets. We've done some of this already, but we need to do more.

➢ *Developing a focus on results based on value-added information and processes.* The demands of the Information Age mean that NSA must determine how to provide information to our customers that is more valuable than that they can get from CNN. That is, we have to use SIGINT analytic insights and judgments to enhance and explain information that may be widely available through open sources. We must produce core secrets, information not available in open sources, e.g., plans and intentions. We have to be decisive. We have to take risks, stick our necks out, and provide to our customers interpretations that reflect our corporate knowledge and expertise in a way that is meaningful to them and meets their information needs.

~~(FOUO)~~ The articles in this issue of CRYPTOLOG address most of these areas. They also acknowledge a critical fact: that the real impact of technological change is in human terms. That is, how NSA professionals will take advantage of new technology to understand and cope with that technology as it applies to their SIGINT and INFOSEC missions. The articles contain several important common themes: the need for change; the importance of continual training; and the growing need for cross-organizational teaming.

P.L. 86-36

~~(C-CCO)~~ I'm pleased to note the discussion in these articles of many important efforts already underway. The reengineering of the Cryptanalysis Career Field, for example, described by [redacted] and [redacted] is very encouraging. Recognizing the problems caused by the reduction in Agency hiring at [redacted] Its new focus acknowledges the need for multiple skills, provides for multidisciplinary training, and encourages interaction between specialists in subdisciplines like mathematics, engineering, and analysis. New professionalization criteria are being developed as part of this process. Striking a similar note, Bill Nolte compares modern cryptology to the medical profession in which all the participants are critical to a successful outcome.

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

~~(FOUO)~~ The overall impression left after reading these articles is that NSA professionals are working hard to figure out ways to deal with the many technological challenges we're facing. Typical of the optimistic and can-do attitude that has characterized NSA for years, our workforce is taking on these new challenges, too. The challenges are difficult, but people are clearly not discouraged and are developing new and creative approaches to the problems at hand.

~~(FOUO)~~ To me this means three things:

- We need to pursue the improvement of internal NSA core processes. We have begun to address this area in the process-improvement activities now underway. Teams have been established to identify root problems and recommend future courses of action for both SIGINT and INFOSEC. Clearly, we have to focus on the insights these teams develop and respond with improvements that will allow the Agency to be more streamlined and flexible in the future.

- We need to encourage cross-organizational and cross-disciplinary teamwork. We all recognize the benefits of such collaboration and can point to many examples where such teamwork has paid off. We need to examine the reasons why such teaming does not occur routinely, and then make changes as necessary to ensure teaming becomes a routine and accepted business process at NSA.

- We need to reduce bureaucracy so we can more rapidly take advantage of new information technologies to improve our SIGINT and INFOSEC missions. In today's climate of continuing technological advancements, we must find ways to reduce cycle times or risk becoming irrelevant.

~~(FOUO)~~ All these improvements are well within our grasp. We can enhance the organizational and institutional processes for SIGINT and INFOSEC and thus allow our workforce to take advantage of new information technology to do their jobs better. We can overcome traditional resistance to teamwork and optimize the synergistic efforts of the entire workforce. And we can institutionalize technological flexibility to ensure we continue to evolve with new technologies, in both a mission sense and a support sense. We can and we must do these things to keep up with the pace of change. Perhaps our vision ought to be: "The Universe is Subject to Change at Any Time . . . And It's Right on Schedule."

Kλ

Signals Collection Career Panel Update: A Look at Some Goals

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

by Ken Williams, B46

~~(C)~~ The Signals Collection Career Panel (SCCP) is taking a hard look at its future and evaluating the viability of the career field as we presently know it. [redacted]

~~(C)~~ Although the study is still in progress and the final recommendations are not completed, we do believe that the efforts to affect positive changes over the past decade or two have been more reactionary than planned and at best have only been cosmetic in attempting to make distinctions between hands-on collection and collection management. Although always a tool of the collector, the realities of personnel draw-downs may force the latter function to be subsumed by the Intelligence Analysis discipline—particularly if the Analyst-Driven System comes to fruition.

[redacted]

~~(C)~~ Whatever is the ultimate solution, greater cooperation and effort must be achieved in joint sponsorship of this program among all concerned parties whether they be a career panel, producers or consumers. The only way to achieve technical excellence—to improve the technical ability and leadership of the individual and to ensure the technical health of the organization—is to form a partnership between management and the technical support infrastructure. The developers must be sensitive to the requirements of the target analysts and management must demonstrate its vested interest in the technical workforce by maintaining positions, providing training, and rewarding achievements.

~~(C)~~ The SCCP has had an extensive partnership with the National Cryptologic School and has supported E4's efforts to develop, upgrade and expand its Signals Collection curriculum. A representative of E4 sits as a full member of the panel and, along with the panel execs, has helped to support a very outstanding advanced technical training program—to include the very latest in computer based training techniques.

~~(C)~~ Among other efforts, the SCCP will be working directly with the DO THAB to expand its Advanced Collection Officer Development Program (ACODP) to satisfy the newly established requirements of the Agency's Technical Development Program (TDP). *Some proposed improvements include the resurrection of the Signals Collection Intern Program, the expansion in advanced collection training, identifying more Titled Tech Track positions, developmental job assignments, cross-discipline team projects, technical conferences, one-on-one mentoring/tutorials with senior technical experts, etc.*

~~(C)~~ As you can see, the SCCP is committed to improving and maximizing the Agency's overall technical health through new and improved approaches and programs. It will also strive to ensure that the technical workforce is properly trained, motivated and challenged and that continued development and performance in the technical track be properly recognized and rewarded—to include incentive pay for those hands-on collectors. We must never lose sight of the fact that without collection, this Agency cannot produce SIGINT. We must nurture this critical skill field and those in it. The SCCP will keep all concerned apprised of our progress.

Kλ

> Cryptology will only be effective if it stays close to the evolving new problems and opportunities. Cryptologists are going to have to be actively involved with collection, [redacted] we must develop mechanisms for bringing teams together across organizational boundaries and identifying the leaders who will be able to coordinate the talents of a team. We also need to control the parochialism which is rampant at NSA and which often stifles or prevents communication across organizational boundaries. A solution to this problem will require a major change in NSA's managerial mindset.
>
> *— Recommendation of the Deputy Director's Cryptology Futures Study*

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

P.L. 86-36

Signals Analysis: A Cornerstone for the Future

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

by [redacted] *E543*

~~(C)~~ In the past, many Signals Analysts have been technicians, trained to perform a sequence of actions to process taped intercepts. However, Signals Analysis is evolving into a cornerstone profession at NSA. The Signals Analysts of the future will be in a position to make significant contributions to the Agency's mission by focusing collection on critical targets, adjusting to the impact from the modern communications technologies, and taking an active role in managing the large volume of data that could be intercepted in the future.

Focusing Collection

~~(C)~~ ***SIGINT is moving away from a Data-Driven System, and, in the continuing days of doing more with less, Signals Analysts will allocate scarce resources in proportion to the intelligence payoff.*** Future Signals Analysts must take a proactive role to ensure an effective Analyst-Driven System. [redacted]

[redacted]

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

Kλ

CRYPTOLOG
Issue 1 1999

Mathematics: Reaching Out in Space and Time

by [redacted] Z31

(~~C-CCO~~) Cryptologic mathematics is both a mature discipline, solving incredibly hard Agency problems every day, and simultaneously a youthful, uncertain beginner facing a new world of challenges. The mature capabilities for analysis and design of cryptography, and a host of other mathematical problem-solving functions at NSA, are powerful, success-driven, treasured. Despite the confidence that this success justifies, mathematicians are rapidly learning that they face an unfamiliar, changing world which does not respect many of their assumptions about what mathematicians do, and that they must change with the world—just as every other discipline at NSA is being forced to change.

[redacted]

(~~C-CCO~~) A second, fundamental aspect of mathematical success is the tool-building that has accompanied classical analysis. The structures involved were modeled and generalized, tools were built which worked on the next problem as well as the last one. An immensely powerful tool-kit has been built up over the years.

~~(C-CCO)~~ Last, but no less important, success has followed because mathematicians have shared these tools with each other. There has been a very strong sense of community, common training in a relatively stable course of theory and practice, healthy production and wide dissemination of publications, lots of seminars and conferences, reasonable movement among organizations, fresh talent recruited to renew the supply of ideas.

(U) Even so, with all this going for them, mathematicians still find themselves in a world changing too fast for anyone to be complacent.

[redacted]

[redacted]

(U) One result of these efforts is an increasing number of mathematicians reaching out to learn from and work with other organizations and disciplines. This trend must not only continue, but expand, to meet the problems we are already seeing. It can only be hoped that management in these related organizations will encourage such contacts, awkward as they may sometimes be under existing boundaries.

~~(S-CCO)~~ Mathematicians are learning where the mathematics is in these new contexts, applying the tools they have, and starting to develop new ones. It is impossible to predict what sorts of advanced mathematical tools will be developed here in the coming years. But the glimpses we have already had of the mathematics needed to address our new challenges clearly indicate that these too will contain and motivate sophisticated, classical mathematical analysis. Depth of research and knowledge in the discipline are proving essential in the new world as well as the old. In fact, the problems and mathematics are just plain getting harder all the time. The combination of this tradition of and need for subject matter depth, with the inspiration of new, hard problems, should generate extremely productive mathematical tool-making.

(U) On the worry side, there is some concern for the health of the mathematical community that has contributed so much to the discipline's success over the years. For one thing, it is not as easy as it once was for a mathematician to move around NSA, spreading and learning new ideas with each new office. Conferences and published papers are not enough: professional development requires extensive work on a variety of problem sets, with a variety of people. For another, diminished hiring diminishes the flow of new ideas and ways of thinking into a field which lives or dies on creativity. Thirdly, it is proving difficult to keep training up to speed with the new material mathematicians are learning or wanting to learn. Mathematicians have generally recognized how much their success depends on the strength of their community. In this stressful time, they must not forget to devote the time and energy needed to keep this community alive and well.

(U) Because of the ferment described above, rather than despite it, mathematics at NSA will prosper in the coming years. It offers powerful tools and well-developed tool-making and tool-wielding experience, no less applicable to tomorrow's problems than today's. But mathematicians also know that they cannot rest on their laurels. And though they have never been off in a corner by themselves, no matter what the stereotype, they realize even more clearly now that they share the same fate as all other disciplines here: work together and succeed, or fall dangerously behind.

(U) *The author wishes to acknowledge a debt to material and themes contained in the 1993 Report of the Deputy Director's Cryptology Futures Study Committee, chaired by* [redacted]

Kλ

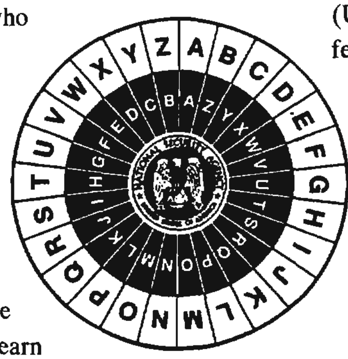
P.L. 86-36

CRYPTANALYSIS CONFERENCE, 1994

by [redacted] Z211, CACP Chairman

P.L. 86-36

~~(FOUO)~~ Two critical issues were addressed at the 1994 Cryptanalysis Conference. One was the exciting trend in communications which threatens to reshape our discipline: in what directions are we moving, what problems require our attention, and how have cryptanalysts been successful in analyzing new forms of data? We were fortunate to attract a set of technical speakers who are blazing a trail into this uncharted territory. By sharing with us their experiences, they prepared us for some of the challenges which lie ahead. We also heard overviews from [redacted] who were among the first to envision the revolution which is now upon us.



(U) The other critical issue deals less with the acquisition of individual skills than with the identity of Cryptanalysis as a community. Each of us recognizes that our career field is undergoing rapid transition, and that we must be willing to confront new problems and learn new skills. None of us came to the Agency with academic training in cryptanalysis, so we all have willingly travelled this path before.

~~(FOUO)~~ When we first acquired our cryptanalytic skills, we were regarded as the wizards of the Agency, treated with respect for having accepted a lifework which demands great creativity and offers rewards only seldom. Where do we stand today? Stung by the Agency's unwillingness to hire into our profession, many of us are asking what we should do to revitalize our career field, to restore the place of honor it once deserved.

(U) The Career Panel selected about 70 cryptanalysts to provide advice on these and other issues. We tried to choose many of those whom we expect to be providing our cryptanalytic leadership as we enter the next century. Videotapes of the technical talks are available from the Panel office. The exciting group discussions provided hours of passionate, but always respectful, debate.

(U) The unmistakable conclusions of the conference: cryptanalysts are extremely versatile, willing to adapt themselves to meet any challenge, and they work very well together and with others. Our destinations may be uncertain, and our paths will certainly diverge, but our wills are strong. We will travel many productive miles together.

~~(FOUO)~~ The essay which follows provided only the kickoff for a stimulating two-day conference. Also included here is a report on the popular and pivotal group session organized, and introduced separately, by [redacted] entitled "Reinventing Cryptanalysis." The ideas which arose at that session will form the central theme for this year's Conference, scheduled to be held at SRC, 29-30 March 1995. The functions of cryptanalysis are expanding rapidly, and the Panel is contemplating a very substantial revision of its criteria to encourage the development of the additional skills which will be required to cope with our altered environment.

P.L. 86-36

Opening Remarks

by [redacted] Z211, CACP Chairman

(U) Good morning, and welcome to the Cryptanalysis Conference, 1994. We are greatly indebted to the Supercomputing Research Center for hosting this conference, as they did last year. Those of us who were here last year are aware of the superb job which the SRC management and staff always do to assure our comfort.

(U) Each of you has been personally selected by the CA Career Panel because we regard you as a key player within our Community. It is a measure of the respect we have for you, individually and collectively, that we have invited you to provide advice, inspiration, and support in our continuing effort to supply the Agency with the best cryptanalysis we can.

(U) These are critical times for Cryptanalysis. Recently organized into a centralized homogeneous Group, we find ourselves enmeshed in the swirling eddies of upheaval, as our sphere of action undergoes unparalleled transition. The cryptanalyst whose methods are limited to colored pencils and "Military Cryptanalytics" is no longer able to contribute effectively to solutions of Agency problems. Each of us needs to be familiar with the capabilities of contemporary computers and must be able to assess both quickly and accurately the speed and the memory requirements of potentially useful cryptographic algorithms.

~~(C)~~ The explosion in computer technology has drawn worldwide attention to the need for security in the transmission of data, with the result that cryptology has outpaced cryptanalysis. The difficulty of our problems has grown much faster than our ability to reduce the resulting cipher to plain text. There was a time, not so long ago, when communications security might well have been sacrificed or compromised in the interest of speed or accuracy, but today our targets can enjoy both security and convenience, with a wide choice of implementations from which to choose.

(U) Cryptanalysts justifiably take great pride in their flexibility. Uniquely among Agency professionals, cryptanalysts have acquired skills which do not come merely from textbooks and are not the subject of university courses. No other professionals could face the impending unrest in their discipline with the confidence we have that we can invent or acquire the new methods necessary to solve important Agency problems.

[redacted]

(U) Each of us has learned a valuable lesson from that experience. Versatility is essential; variety of exposure must be encouraged. Cryptanalysts and mathematicians are uniquely privileged with the opportunity we have for Agency job rotation. We must avoid stagnancy and constantly seek to broaden our spectrum of utility.

~~(FOUO)~~ The single most critical issue which confronts Cryptanalysis today is the lack of hiring. Because it is not a university subject, cryptanalysis is not on the "critical skills" list. We have been unable to achieve recognition from upper management that the stock of cryptanalysts, depleted by retirements, needs replenishing. This is a very favorable time to be hiring—because of the difficult economy, excellent candidates are available—but we have been denied a license to hunt. Perhaps our greatest need is an algorithm, inexpensive to implement, which could be used to identify recent college graduates who have the potential to become productive cryptanalysts. Until hiring is restored, cryptanalysts may explain its absence in any of three ways: (1) maybe cryptanalysis is a dying art form, and we are just slow to leave the sinking ship; (2) perhaps our skill levels are regarded as being so high that we are expected to cover for those departed; or (3) the obvious reasonable explanation is that the very able mathematicians whom we have been hiring will drift into cryptanalysis and will perform well enough to fulfill our obligations. This explanation many will find unsatisfying, maybe even dangerous.

> ***The single most critical issue which confronts Cryptanalysis today is the lack of hiring.***

~~(FOUO)~~ Inevitably, our position will be contrasted with that of the mathematical community at the Agency. Mathematicians are multiply blessed. They have benefited from a strong hiring posture, now stronger qualitatively than ever, and their support systems, starting with their immensely successful Cryptologic Mathematician Program, have been the envy of all other career fields. Central to their success has been the magnificent support supplied by the Institute for Defense Analyses.

~~(C)~~ The trend toward the use of mathematical principles in the design of sophisticated cryptologic devices has conferred a substantial advantage upon the mathematically trained cryptanalyst. Those of us who lack such a background have good reason to admire the successes that our mathematically trained colleagues have enjoyed. But admiration can be accompanied by frustration. As our mathematical arm grows strong, must our non-mathematical component wither? This is an issue which deserves an honest assessment.

~~(S)~~ The good news for those of us who lack a strong mathematical capability is that cryptanalysis is expanding in another direction. There are explosive changes in communications which will have aimpact heavily upon both the science and the art of cryptanalysis. Much more of our resources will need to be devoted to preparing new intercept for cryptanalysis. We have far too few people who are facile at this task, and it is one which requires substantial ingenuity. Cryptanalysts should be ideally suited to function successfully in this newly developing area. They know best what form the analyst needs data to take, and they know exactly what information must not be overlooked. I see no mathematical component in this new technology. The keynote talks by [redacted] and [redacted] and today's seven technical talks have been selected to show how classically trained cryptanalysts have solved problems which lie on the border of this new frontier in cryptanalysis. I look forward with great excitement to a glimpse at the future of our discipline. I am convinced that this is not a redeployment of the cryptanalytic workforce, but is a genuine broadening of our field as cryptographic usage changes to include high-speed devices. It is clear that there are big victories to be won, and we must be quick to seize our opportunities.

While hiring may be largely beyond our control, training should not be. If we need exposure to new cryptologic ideas, and we certainly do, we'll need to do it ourselves.

~~(FOUO)~~ Closely allied to the infusion of these new ideas from telecommunications is the need for dissemination of information at all levels. While hiring may be largely beyond our control, training should not be. The cryptanalytic staff at the National Cryptologic School is woefully under strength, and cannot be expected to expand soon. If we need exposure to new cryptologic ideas, and we certainly do, we'll need to do it ourselves. Perhaps in conjunction with Tech Track, a way must be found to make the development and presentation of unfamiliar material an attractive alternative for that huge majority of us who are typically extremely reluctant to leave our current exciting crypt challenge. This inertia, natural as it is for those of us who love our jobs, has become a Community problem. Most cryppies are unwilling to give talks and write papers. We are just not activists. Tomorrow's workshop on "Sending the Public Service Message" will consider how to reverse this trend.

~~(FOUO)~~ I once thought it would be a good idea to institute a Master's program in Cryptanalysis, leading to something like a "Master of Cryptanalytic Arts" offered by the National Cryptologic School. But more sober reflection led to the conclusion that such a degree would likely be won only by perennial classroom students, which includes very few cryppies. Classical education may well be inappropriate for teaching (and learning) cryptanalysis. We hope to learn a great deal from today's timely presentations; waiting until a slick course could be prepared would place too many of us too far behind. We need solutions for our current inability to spread cryptanalytic knowledge, and one of our working groups tomorrow deals with "The Training Challenge." We cryptanalysts are overwhelmingly introverted. Few of us desire to appear before a classroom, even a classroom of our colleagues. Many of us have sufficient initiative to learn for ourselves what we need to know, but something must be done to provide information to our less experienced coworkers who don't realize their deficiencies, and who could become greatly more productive with timely education.

P.L. 86-36

~~(C)~~ Communication poses problems for us in other ways. It was easier for us to show others the fruits of our labors when we were spread across the Operations Directorate. Now we have allowed our sphere of influence to diminish, with the result that our accomplishments are now made known to a much smaller audience. We need to publicize our triumphs to those who could use our expertise. One of tomorrow's sessions, "Marketing Cryptanalysis," will go into this concern in more detail.

~~(FOUO)~~ There is another negative result of our concentration within a single Group. I am not being immodest when I say that cryppies are smarter than many other Agency communities. A comparison of academic records alone is enough to convince anyone of our intellectual capacity, and each of us has gone far beyond our original academic training. But it is unfortunately unrealistic to expect that we will receive promotions at a deservedly increased rate, since bureaucracy decrees that benefits be spread uniformly across organizations.

~~(C)~~ At last year's conference, a number of problems were discussed dealing with issues of morale. Our management should be extremely proud that few of those problems remain. I would like to identify one problem which I think will eventually cause difficulties for us: that is the plight of those among us who have moved away from a purely technical career to deal with the challenges of management. The number of SCES positions is extremely limited and is unlikely to expand. Within Z Group the problem is extremely acute, because our SCES positions are, or soon will be, occupied by very bright and relatively young leaders who seem unlikely (because of the separation of cryptanalysis from the rest of the workforce, and because of the difficulty that cryptanalysts seem to have in entering higher management) to move from their posts in the near future. Also, most of our Office-level managers have been chosen more for their technical excellence than in recognition of their managerial prowess. In short, I would expect any management-oriented cryppie to be very discouraged by the current prospects. Should we do anything to reverse the rising trend of technocracy?

~~(FOUO)~~ This conference presents to your Career Panel a vital opportunity to hear what issues are important to you, our fellow cryptanalysts. The advice and consent which we get from you in the next two days will guide our actions throughout the year. Last year's conference, though times were certainly tough, revealed the cohesion of our Community, the unity and the spirit that helps us move toward our common goals.

(U) So welcome to the 1994 Cryptanalysis Conference. Each of us will find strangers here—but strangers who share our goals and our burdens. I look forward eagerly to meeting those of you whom I do not know. In these two days, we gather to learn from each other, to share with each other, in the hope that each of us will benefit from what we see and hear, and that we will return to spread our new knowledge throughout the Community.

Reinventing CA: A Brave New World for the Career Field

by [redacted]
CACP/Z21

P.L. 86-36

~~(FOUO)~~ Last year's CA conference had as its central theme the role of the cryptanalyst in the modern, post-Cold War, post-reorg world. If you examine the conference speeches, you can pick out some of the issues which led the CACP to call for a hard look at our discipline. New technologies, austere hiring, an apparent contradiction in what outsiders and insiders considered to be cryptanalysis: these realities seemed to be pushing the classical cryppie into the margins of the cryptanalytic establishment, while the latter appeared to be becoming synonymous with the crypto-math community in the eyes of much of the Agency.

Perhaps not surprisingly, the working group stressed the importance of training in related fields.

~~(C)~~ The 1994 conference organizers worked under the assumption that the "ca vs. CA" distinction which I defined in my speech was a valid one, and the conclusions that the "reinventing ca" working group reached seemed to support the perpetuation of that distinction. (For those for whom this is new, I defined "ca" as what someone professionalized in cryptanalysis is trained to do and "CA" as what Z group does.) In its report, the working group defined CA as "the diagnosis and exploitation of data which is, otherwise, not obviously intelligible." Then it went on to carve out a little niche for the "classical" cryptanalyst in diagnosis and exploitation, simultaneously stressing the importance of training in related fields. This is, perhaps, not surprising. We organizers stacked the conference with talks that showed how classically-trained cryptanalysts could be successful in what we termed "modern" cryptanalysis. We believed then that the way forward was to create a distinct identity for ca that would place it on an equal footing with the other disciplines that were involved in doing CA.

P.L. 86-36

~~(FOUO)~~ It took several months for the conference report to come out, and even longer for the Panel finally to put the report on the agenda for discussion. In the meantime [redacted] began his term as Panel chairman. Dan's first initiative was for the Panel to go to the Office Chiefs and Chief, Z and ask their advice on what the CACP could do better to support the activities of their areas. These interviews were extremely enlightening. Another important thing happened during this period; the CA intern program looked like it was on the chopping block. With no hiring and all those empty billets, there was a distinct possibility that we might have to close down. Here [redacted] came to the rescue, suggesting that Z group might benefit by hiring computer scientists and engineers (these are, with mathematics, the relevant critical skills for CA) and training them through the CA intern program. There is still no hiring, but at least there is a plan.

~~(FOUO)~~ By November it was clear that the Panel could no longer operate without a cogent working philosophy of the nature of cryptanalysis. The Panel had promised the community another conference in January, but as we wrestled with the issues confronting us, that conference seemed ill-timed and more and more irrelevant. At long last, in early December, the CACP held an offsite to synthesize the input we had received from the 1994 Conference, Z-group management, and from studies like the "Future of Cryptology." The conclusion of this day of soul-searching was to me as clicking the ruby slippers must have been to Dorothy: *cryptanalysis is Cryptanalysis*. We always had the power, but we had to find out for ourselves.

~~(FOUO)~~ Simple as the concept is, the implications are far-reaching. Z-group cryptanalysis requires the efforts of people in many sub-disciplines. We, therefore, began to try to fashion a career field that would be as relevant to newly-hired mathematicians, computer scientists and engineers as to those in non-technical fields. In the ensuing months we have constructed new criteria for the field which attempt to ensure that every cryptanalyst will have a thorough grounding in the classical subjects: diagnosis, cryptography, related fields, but will also enable him to contribute in the areas for which his academic training has uniquely prepared him. While last year's conference spotlighted how the classical cryptanalyst could move into areas of new technology, this year's gathering will focus on how to embrace diverse technical backgrounds to strengthen cryptanalysis. The new criteria for professionalization in cryptanalysis are a work in progress, and will be a major topic of the conference. Here is what they look like so far.

~~(C)~~ A number of the requirements will seem familiar on the surface. We will still require three years of creditable experience and we will still require a paper and a program. The omission of the PQE from this list is not accidental; an aspirant's grasp of essential knowledge will be assessed in other ways. We will require work experience in three core areas: exploitation, diagnosis and related fields, communications and collection. We will also require two elective tours, to be negotiated with the Panel execs. As an example, a mathematician might elect tours in attack development or algorithm design; an engineer might choose to do hardware reverse engineering or signals analysis; a computer scientist might work on CAPRI or study computer networks; a non-technical aspirant might delve into book-breaking or bit-stream analysis. We're not attempting to pigeon-hole anyone here—the mathematician could do book-breaking and the anthropology major algorithm design—the point is rather in the explicit inclusion of what was previously considered peripheral into our new vision of the career field.

~~(C)~~ Training requirements will be completely revamped, and this will necessitate a great deal of work in course development. Again, we envision a core of required courses and a wide choice of electives. The core will contain some new courses on which we hope to get started at the Conference: a related fields survey course, a "foundations of CA" course which will survey the most significant cryptographies extant, a new diagnosis course which I like to call "patterns of thinking," and a "topics in math, CS and engineering" course that will highlight the ideas in those fields with the most important implications for cryptanalysis. Some of our present required courses will become electives. Does everyone need to know how to solve a grille transposition? Probably not, just as we don't all need to program digital signals processing (DSP) chips—yet.

(U) The Panel is immensely excited about this new direction for the career field, even if that excitement is tempered with apprehension about the hard work necessary to get this new program off the ground. We hope we can count on your help and your counsel as we take cryptanalysis into the next century.

Kλ

Linguists and a Changing Future

P.L. 86-36

by [redacted] *Language Career Panel*

~~(S-CCO)~~ We linguists are facing a future about which we know little beyond the fact that our environment is changing. We will need to learn new non-language skills, learn new languages and dialects, and sustain language expertise. How do we meet these challenges? The Agency has focused its resources for the past 30 years on developing professional linguists, and it has succeeded. The Agency language population presently consists of approximately 75% certified linguists, a turn-around of significant proportions in demographics over the past 30 years. The future requires that we focus resources on post-professionalization. The Technical Track Program offers us linguists a way to mobilize and maximize resources to cope with the future. It enables the Language Career Panel, Technical Health Advisory Boards, and other Agency organizations and institutions to identify opportunities, establish requirements, and implement courses of action.

~~(C-CCO)~~ The Language Career Panel Staff conducted a study several months ago of the training profiles of over 350 certified linguists who had joined the Technical Track Program at that time. (At the present time, over 450 linguists have joined the program.) The results were alarming. Since 1990, these participants in the program had spent from one to three percent of their annual working hours in any career-skill training or educational endeavors, as registered in Agency records. The percentage was similar for applicants to the Senior Technical Development Program.

~~(C)~~ Is there a lack of post-professional programs for linguists? While the Directorate of Operations' Senior Language Advisor and the National Cryptologic School have created and funded numerous programs over the years to enhance the skills of certified linguists, it is true that many certified linguists have not applied to these programs because the programs did not coincide with their personal and mission needs. It is also true that training funds are limited and are prioritized to go first toward the training of linguists up to the beginning professional level; thus, post-professional opportunities are limited. Other linguists believed that they did not need to develop their skills except through on-the-job experiences. Still others have developed their skills through personal endeavors outside of the Agency; these endeavors have not been registered in Agency records. Regardless of the reasons, certified linguists have not been pursuing registered post-professional training, educational, and development opportunities, which would conceivably have enhanced their language career-field skills.

~~(TS-CCO)~~ If we do not pursue ways to improve our skills and productivity, we shall find ourselves faced with events and circumstances to which we may not be able to respond. Since the Agency will not be hiring linguists in any large numbers, we shall have to rely on our own talents to meet future challenges. In addition to sustaining language expertise and learning new skills, we could accelerate the development of non-certified linguists through intensive mentoring programs, educational and training seminars, and as members of the Adjunct Faculty. The present population of language aspirants is experiencing difficulty in passing the Professional Qualification Examination. We can assist the Service Cryptologic Elements in enhancing the language proficiency of military linguists beyond Level-2 proficiency to cope with the expected future higher-level communications at the Remote SIGINT Operations Centers and elsewhere. There are presently about 900 USSID-4000 military linguists, 13 of whom are certified and approximately 200 are aspirants for professionalization. We need to forge a partnership with the SCEs to address the future of language work and proficiency. Cross-training programs can augment the language work force and shift resources to meet critical-language requirements. To improve the skills of military and civilian linguists, we need to learn and develop interactive computer-aided tools, conduct language seminars, and establish extensive mentoring programs.

(U) Extensive mentoring programs may alter the way in which many of us have previously gone about our business. Master linguists, for example, could provide career and skill-field advice and guidance to Senior Member and Member Linguists, who, in turn, could guide and develop junior linguists toward professionalization. Extensive mentoring programs would require more emphasis on skill development and less emphasis on mission. The goal, of course, would be the linking of skill development and mission needs. Management would need to permit linguists the time to sustain language skills and learn new skills. We linguists would need to focus attention on flexibility in the work place and adapt to sudden changes in circumstances.

~~(FOUO)~~ Because of the nature of our work and security constraints, we must guard against becoming insulated from ideas, concepts, and technology pursued outside of the Agency. We need to join academic and professional societies and assocations and subscribe to related journals and newsletters to keep abreast of national and international innovations and initiatives, and describe or introduce these innovations and initiatives at the Agency whenever it would be feasible. Attendance and participation in conferences and seminars can also expose us to new ideas, concepts, and technology.

~~(FOUO)~~ We shall expect to increase productivity, anticipate and cope with future events and circumstances, and learn new skills. We must, however, also find time to maintain language expertise. As of this writing, several post-professional opportunities and plans, all under the auspices of the Technical Track Program, have been developed. The DO/SLA has developed a mechanism which will identify conferences and seminars, select the appropiate individuals to attend them, and provide the funds for these individuals. The Language Career Panel has developed a draft of a Resource Guide for linguists in the Technical Track Program to use to develop their careers. The Panel recently proposed to the Senior Technical Track Board the establishment of expanded mini-immersion programs tailored to the personal and mission needs of linguists. Many other ideas are in gestation. The THABs, for example, are exploring the idea of creating positions within the Key Components primarily for the career development of selected titled linguists.

~~(C-CCO)~~ Future programs will be derived from ideas recommended by linguists who are participants in the Technical Track Program. Ideas are limited only by our lack of creativity and the shrinking federal budget. The Language Panel has created and implemented an electronic subscription network to keep titled linguists informed of activities, opportunities, ideas, etc. The subscription network has already generated responses and ideas. The Technical Track Program is geared to provide certified linguists with a means to develop their own careers to benefit the Agency as well as the linguists themselves. In the final analysis, each of us must take full responsibility for developing our individual careers in a way that will meet our personal as well as mission needs. The Technical Track Program will evolve as we all cope with a changing future.

Kλ

We must begin now by involving as many from the cryptologic workforce as possible in the process of working horizontal problems across skill field and organizational boundaries. We need a workforce of experts in various fields who are used to working together with others outside their field. We must also identify the technical leaders and give them the opportunity to learn how to provide the unique form of technical management that will be needed to guide these cross-disciplinary and cross-organizational teams.

— Recommendation of the Deputy Director's Cryptology Futures Study

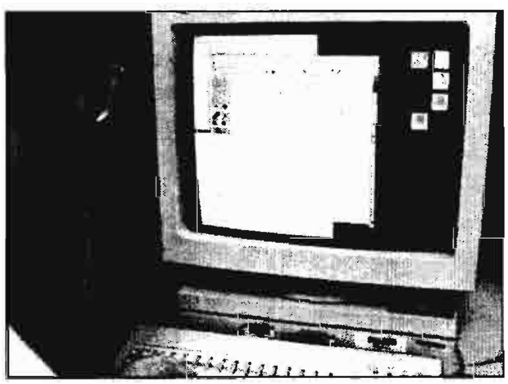
Intelligence Research + Traffic Analysis = Intelligence Analysis

by [redacted] /ACP

P.L. 86-36

(U) Every cryptologic field at NSA has had to evolve over the years to meet current and future demands. Intelligence Analysis is one career field where transformation has been obvious, as two fields, Intelligence Research and Traffic Analysis, were combined to form a new discipline. Driven by exponential expansion in communications technology and rapid political change, the new field must be greater than the sum of the former fields to enable it to meet the changing needs of the Intelligence Community.

~~(FOUO)~~ Intelligence Analysts will continue to play a key role in the production process, but with the incredible growth of modern communications targets and analytic tools available for use by NSA analysts, we have been challenged to understand not just a single aspect of a target, but much, much more. [redacted]



P.L. 86-36

(U) NSA is in the *business* of producing intelligence. That intelligence comes in many shapes and sizes and the Intelligence Analyst of the future must be able to tailor the finished SIGINT product to the needs of strategic and tactical commanders, those interested in economic or diplomatic issues, or those involved in making national policy decisions. If it needs to be presented to the customer through video links, we need to do that; if they want it in on-the-spot reports, we have to respond; if they need a 3-month in-depth study, complete with maps and an effective Desk-Top Publishing presentation, that is another step we have to take to fulfill the customer's expectations. Our SIGINT reporting must continue to be useful, valuable, responsive, and top-notch!

(U) How much does this say about the future? Mostly that Intelligence Analysts need to adapt, to know our customers, what they think, what they want, and how they want it. Sound unpredictable? It is. That is why it is essential to be flexible, to be in tune with the unique needs of each of our users, and to stay abreast of new technologies. The benefits of teamwork will become more and more evident in this environment; cooperation between individuals, between teams, between offices and groups, must occur. The field of Intelligence Analysis ensures a breadth of knowledge that will "make" the leaders who understand the macro view. These same leaders will also have the technical competence to know and understand the specific analytic techniques that should be applied to solve our future challenges.

Intelligence Analysis:

Production and Reporting in a Changed Environment

by [redacted] P054

P.L. 86-36

~~(C)~~ [redacted] has described one of the several fundamental changes reshaping the Intelligence Analysis career field and its operating environment: the changing shape of the world's communications. Concurrent and equally fundamental changes in the political environment in which SIGINT and its customers must function, and in the relationship between open-source information and "secret intelligence," compound the transformation taking place around us. In rounding out a look at the future of intelligence analysis, we need to examine the impact of those other revolutions.

American Intelligence in Peacetime: A Contradiction in Terms?

(U) For the first time in half a century, the United States is not engaged in real or virtual war. How will the American people respond to that? The evidence of the first five years of the post-Cold War era suggests that traditional American concerns about "foreign entanglements" have not disappeared. The evidence further suggests, however, that the American public that emerged from the struggles of the past five decades recognizes, better than previous generations, that U.S. involvement in world affairs cannot be episodic or intermittent but, for better or worse, is permanent at some (possibly erratic) level of national attention and expenditure. However painful the adjustments of the past few years have been, comparisons with previous "demobilizations" after the First and Second World Wars support the case for maturity.

(U) Within this consensus, it is at least reasonable to suggest that the American people will accept the reality of a permanent, peacetime intelligence establishment. They will not, it is clear, support this establishment at wartime levels, nor will public opinion permit any of the national security components—foreign affairs, the military, or intelligence—the operational latitude that comes with the survival issues attendant to war. In the post-Cold War era, the national security structures will be held to higher standards of stewardship of both the public purse and the public trust. The military and foreign affairs establishments will be required, each in their own way, to confront public controversy about their size and roles; the intelligence community will be asked to deal with the particularly strong American ambivalence concerning secrecy and "espionage" as consistent with our national values.

~~(FOUO)~~ The effects of this change are about us already. For an agency that spent its first four decades heavily tilted toward securing its sources and methods (understandable in an agency where results point to a single set of sources and methods), complying with the reality of "openness" will prove a difficult task. We are sailing a very large ship through a very narrow channel. The hazards of excessive disclosure, with which we have traditionally dealt, continue; the hazards posed by a failure to demonstrate our value are no less real. One thing is clear: we are a long way from "No Such Agency," and there is no turning back.

~~(S-CCO)~~ As the final stage of any given cycle in the cryptologic process, the stage most proximate and intelligible to the consumer, reporting and dissemination (intelligence production in the language of the Intelligence Analysis professionalization criteria), cannot be seen as anything less than a critical, integral stage of that process. In an age when the final assessment of our value will come from the consumers of our products and services, it becomes vital to serve those consumers well. When I suggested some years ago that cryptology had to be defined to encompass this function, one of the published rejoinders concluded that "bulldozer operators may be needed on the periphery of archaeology, but they are not archaeologists." Reporting and disseminating effectively the results of our collective efforts are not peripheral to the success, even the survival, of this enterprise over the next decade. They are central to both.

If Peter Arnett is on the Scene, Can Intelligence Be Far Behind?

~~(FOUO)~~ In serving our consumers, we will not only be required to demonstrate value comparable to that received from the other intelligence "INTs," but with that received from open sources as well. During a

Gulf War briefing by a collection of intelligence analysts to the Senate, one Senator, impatient with the number of times he had heard us say that some information could not be provided in that particular setting, walked out muttering "I can get better information on CNN." A particularly brave member of the briefing team chased the Senator down the corridor to refute that contention.

(U) But the presumption remains among significant portions of the public that we are an expensive duplication of the public print and broadcast media, of universities, and of think tanks. We had better be able to deal with that presumption, not just by sneering at it, and not just by pointing to the limitations of open-source information.

(U) The fact is that the value of open source information available to decision-makers has risen, as new communications technologies have come on line and as open-source access to much of the previously denied parts of the world has improved. In large part, this development caused the near-disappearance of closed, totalitarian regimes, and it has accelerated in the years since.

(U) In a world threatened by totalitarian regimes that made information control a central act of their existence, secret intelligence had advantages of access to information no open source could compete with, at least within reasonable, actionable timeliness standards. A researcher at the Hoover Library, working on bound volumes of *Pravda*, was no competition for the intelligence analyst of the 1950s. Once overhead satellites solved the problem of the Soviet landmass, intelligence had a truly extraordinary edge over other sources. (In fact, one could argue that only once before, in the cryptologic successes of the Second World War, has intelligence provided policy makers and commanders with such an information advantage.)

~~(S)~~ Intelligence retains significant advantages, but not in the way we once did, and not for all the same information. Information technology has altered the rules of information management and fundamentally changed the access picture. Only a few decades ago, Soviet dissidents copied by manual typewriter political tracts or, in a remarkable act of physical endurance and moral courage, Russian novels. Now, regimes and dissidents around the world have access to fax machines, satellite transmitters, laptops, the Internet, and, one sometimes thinks, Ted Koppel's phone number. Even overhead reconnaissance now enjoys only a comparative rather than an absolute advantage over commercially available satellite photography.

(U) How do we compete in this environment? Clearly, not by duplicating open-source information. One of the more difficult but essential analytic tasks of the coming era will be what to concede to open sources. This will be necessary for no other reason than that it will be fatal, in an age of austerity, to be seen as an expensive alternative to the New York *Times*. We must identify and emphasize the information that comes to us (and through us to consumers) uniquely through our sources. Even then, we will be asked to prove, through some calculus, that our information was not only unique but worth the cost of its acquisition. Reporting through intelligence sources information already available in open sources will only demonstrate our ignorance of the open sources. Resource allocators will not tolerate much of that.

CNN: speed, not depth

~~(S)~~ The evidence suggests that we will be able to achieve this objective. While much of the public may equate the Gulf War with the "CNNization of information," a small minority of participants, prominent among them Messrs. Bush, Scowcroft, Cheney, Powell, and Schwarzkopf, must know that intelligence, prominently including SIGINT, supported their efforts in ways no predecessors have ever been served. It wasn't perfect, but in the real world little is. The alternative to paying for intelligence information would have been payment in lives, and that's a cost the American people will be reluctant to bear.

(U) In the short but eventful interval from 1991, open source information has become more pervasive and more compelling, certainly to civilian policy-makers. The researcher at the Hoover Library no longer works from bound issues of *Pravda*; he or she is making frequent visits to Moscow, interviewing key officials, and staying in touch with a host of correspondents on via facsimile and e-mail.

~~(FOUO)~~ This will force the SIGINT analyst of the future to be more aggressive in knowing and using collateral, both open and classified. It will force the analyst of the future to be more adept at producing "finished SIGINT," defined in this context to mean SIGINT produced by an analyst cognizant of the collateral available on his or her target but identified by that analyst as having value over and above that in the collateral. We should not worry about competing with CNN. Does Cadillac compete with Jeep? Yes and no. Yes, in that there is a finite amount of money in the market to be spent for personal transportation. Yes, in that the technical staffs of each would like to think they are better at their jobs. No, in that the two products attempt to fill different needs in the transportation market and can coexist within their respective niches.

One competitive niche for intelligence must be the ability to alert to an impending event before it happens.

(U) The same holds true in information. CNN and other open sources will have inherent advantages in reporting the "who, what, when, and where" of events taking place in the open. One competitive niche for intelligence must be the ability to alert to an impending event before it happens. We will not achieve this all the time, [redacted] wonderful "signals" versus "noise" analogy still being true. Another will be an ability to give decision-makers unique and deeply accessed information to the "why" question, with all it means in judging future intentions. In intelligence, as in journalism and history, "why" is still the stumbling block. CNN may get a story first; we must get it right.

Another will be an ability to give decision makers unique and deeply accessed information to the "why" question, with all it means in judging future intentions.

~~(FOUO)~~ This does not mean the SIGINT analyst must produce "finished intelligence." In fact, it is hard to imagine, in the environment we are likely to encounter over the next decade, anything less valuable and less defensible than yet another set of finished intelligence producers. But the SIGINT reporting of the next decade must take place in an all-source context. (A small blessing of this difficult transition would be the disappearance of the artificial distinction between "finished" and "unfinished" intelligence. In an age when National Intelligence Estimates routinely include open-source judgments, even judgments that counter those of the Community, it is anachronistic to think the information process is somehow "finished" when an intelligence analyst slaps a classification on a report. The consumer may not consider even a highly compartmented intelligence report "finished" until she has checked for competing views in the press, called a friend at the Kennedy School or Stanford, or scanned CNN.)

~~(FOUO)~~ A final thought on the cryptologic process and the challenge it faces: Any casual reader of the Electronic Subscription Service or other internal bulletin boards will attest to the existence of debates about who's really important in cryptology. Is it the cryptanalysts or the linguists? Tech track or management? And what about critical versus non-critical skills?

(U) All of this is to be expected in an institution experiencing (moderately) hard times. Some of it can even be productive of esprit de corps. Army and Navy, after all, have coexisted in a competitive relationship for two centuries. But within limits; institutions that exceed those limits ("General Short, meet Admiral Kimmel.") are looking for trouble.

~~(FOUO)~~ If we have learned anything in the half century since cryptology emerged from the Black Chamber, it is that this is not a single discipline, but a process. We are more like medicine, an applied process, than a single discipline. In many respects, the break between the Black Chambers and modern cryptology is the invention of traffic analysis, the recognition that cryptologic attack can reveal information of value even when it is successful only in recovering the externals of intercepted communications. At other times, the information of greatest importance to decision-makers has come from unenciphered communications, even though to the purist this must seem cryptanalytically unsporting.

(U) Once we accept the idea of process, however, the goal becomes very simple: to employ the techniques of that process to provide information of value to the consumer. Once we accept the idea of process or system and agree on which components are critical to that process—literally critical, i.e., if any of the critical components fail, the process fails—than the interdependency of the components becomes unarguable. Debating among ourselves whether computer scientists are more important than linguists (one can argue supply and

P.L. 86-36

demand issues, and the compensation decisions that should flow from these, but that is not the same) then becomes a bit like debating the relative value on a surgical team of anesthesiologists versus surgeons. As a patient, my very strong preference would be that both should be competent.

(U) The technical challenges facing the intelligence analysts of the future will be formidable. Anticipating the needs of consumers, converting those needs into requirements for signals intelligence information, informing consumers of what SIGINT can (and cannot) do, integrating those needs into the technical processes of the agency, and employing the full range of dissemination techniques and methodologies in order to get information the consumer on time and in formats that permit the information to be useful rather than academic are among the tasks at hand.

Kλ

The National Performance Review's report on the Intelligence Community made seven major recommendations, each with suggested actions. Since then, significant strides have been made toward accomplishing these recommendations. For example:

Reassess Information Collection to Meet New Analytical Challenges

- The Foreign Broadcast Information Service (FBIS) has completed two exhaustive studies, reviewing its field collection network and examining products and services measured against consumer needs.

- The new INTELINK information system, now in development, promises to facilitate "real-time communication between analysts and collectors."

- CIA and DIA have increased dramatically the number of integrated analytical papers they produce jointly. Joint task forces bring cross-discipline analysts together to work on key issues.

Integrate Intelligence Community Information Management Systems

- A new Intelligence Systems Board (ISB) co-chaired by the Executive Director, IC Affairs and the Deputy Assistant Secretary of Defense for Intelligence and Security was formed late last year to ensure interoperability of intelligence information systems.

- The ISB and the National Intelligence Council have also established an Electronic Publishing and Dissemination Board (EPDB) for developing policy and procedures to allow electronic text exchange throughout the IC. INTELINK, once operational across the Community, will serve as the central focal point for dissemination activities.

Enhance Community Responsiveness to Customers

- Customer advocates or "issue coordinators" were appointed for each of the 16 major issues in the National Intelligence Need Process (approved by the DCI in July 1993), focusing greater attention on individual customer needs. The issue coordinators have recently completed strategic reviews of their assigned areas, involving substantial dialogue with IC customers.

- The IC has made a major effort to bring service closer to customers, including placing additional liaison and briefing officers at customer facilities and greatly expanding electronic connectivity.

Develop Integrated Personnel and Training Systems

- The DCI's Foreign Language Committee has published a "Unified Language Testing Plan" setting Community-wide language proficiency standards. The plan will be implemented this fall with a pilot project in Spanish.

- A vigorous program of inter-agency rotational assignments is now under way.

Improve Support to Ground Troops During Combat Operations

- The IC Battlefield reinvention lab wraps up its final phase this month, with briefings to senior officials. A panel of outside experts has provided support in the activity this year to General Crosbie Saint (USA, Ret.), the lab's coach.

Reprinted with permission from *Quality and Innovation*, the IC Quality Control Newsletter, Vol. 1, No. 8, September 7, 1994

CRYPTOLOG
Issue 1 1995

Signals Research and Target Development: Past, Present, and Future

by [redacted] P054 TARS

~~(S-CCO)~~ [redacted] Signals Research and Target Development has become the focus of much recent discussion. The number of people involved, however, doesn't fully explain the attention this topic has received over the past few years. SIGINT production is a process. Signals Research and Target Development is our latest refinement of that process. This article discusses what Signals Research and Target Development is, where it came from, and where it's going. Through this discussion, it is hoped that the reader can gain an appreciation of the past, present, and future of Signals Research and Target Development.

~~(S-CCO)~~ SRTD: *WHAT DOES IT MEAN?* Three or four years into its existence, that's still debated in some circles. The views are largely personal—different organizational perspectives result in different definitions. This is natural, coming partially from the fact that different organizations' missions vary, but there is a common element among most definitions:

SRTD is a process

Some practitioners partition it into two distinct, but related, processes. Signals Research (SR) is the process of developing information necessary to exploit a signal. Exactly what that information is can be contentious, but usually includes understanding the operating characteristics of a signal of interest (modulation type, coding scheme, encipherment, etc.), the use and implementation of a telecommunications technology which employs that particular signal (or a set of signals), and exploitation vulnerabilities. The other process is Target Development (TD)—taking knowledge developed through SR and using it to develop sufficient insight to a communications system used by a particular SIGINT target to allow reliable access to information of interest. In either case, SR or TD, the process requires application of multi-disciplinary skills (Intelligence Analysis, Crypt-Analysis, Mathematics, Signals Analysis, Telecommunications, Computer Science, Collection Management, and Language). Sound ambiguous enough? Good!

~~(S-CCO)~~ So, that's the loose definition of SRTD. Who does it? First, it's important to emphasize that SRTD is not a career field. The urge to make it a career field was resisted because of the awareness that the SRTD process required the skills and knowledge of several disciplines. As such, there really isn't any title or COSC for people who do SRTD. In fact, while SRTD elements are primarily staffed by Intelligence Analysts, they also rely heavily on individuals from the Signals Analysis, Collection, Telecommunication, Language, Engineering, and other career fields. For the purpose of this article, SRTD "analyst" will refer to any of the individuals who are involved in the SRTD process.

Past

(U) As recently as a decade ago, the networks that the Agency exploited were very different from those encountered today. Civil networks were very static; military networks were dynamic in terms of Standard Operating Instructions (SOI), but used new technology very gradually. These networks were relatively simple: they employed limited modulation techniques and signal bandwidth was fairly narrow; communications were primarily voice and teleprinter, though use of data and facsimile was growing; and network complexity was only moderate.

~~(FOUO)~~ The state of the Intelligence Community was similarly straightforward. We were in the middle of a long-standing and very dangerous Cold War. The U.S. SIGINT Service was based upon structures put in place during WWII, modified only as necessary for the Cold War. SIGINT priorities were clear. Funding to work against our primary adversaries can now be described as generous—we were able to amass considerable human resources, fund what seemed to be a robust infrastructure, and maintain a healthy investment in systems development.

~~(FOUO)~~ These factors combined to make an exploitation environment that was well developed, with resources sufficient to excel. The Agency met customer demands through focused attacks against networks using passive access techniques. Our understanding of the targets and the technologies they employed for telecommunications was superb. A long history of performance established our technical health in nearly all areas of SIGINT endeavor.

~~(S)~~ As a result, monitoring of technology evolution and network modernization was performed iteratively against high-priority targets. Target development was thought of as continuous, performed daily by numerous "U/I" teams (these elements worked against nets operated by users unidentified by the SIGINT system). It was a critical factor in maintaining an understanding of target telecommunications networks and strong technical health among the work force. The primary discipline involved was traffic analysis.

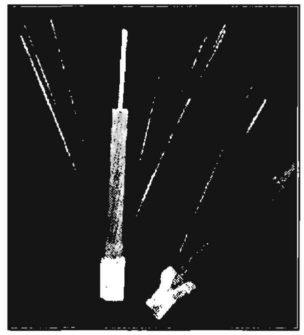
~~(C)~~ The status quo was permanently destroyed by two events: the abrupt overthrow of Soviet leadership, ultimately ending the Cold War and changing world polarization; and the Iraqi invasion of Kuwait and subsequent, massive involvement of global military forces. The first event had drastic and immediate effect on SIGINT requirements and funding. The second highlighted shortfalls in the ability to deal with third-world crises and modern network technologies.

~~(S-CCO)~~ Much of this had been predicted. In the late 1980's, high-level studies (the Perry and Brotzman reports) and several reports written by Agency technical leaders warned of an ongoing technology revolution. They made many recommendations on ways the SIGINT community should evolve. An article in the Fall 1989 *Cryptologic Quarterly* by [redacted] predicted that world developments would force the U.S.S.S. to shift priorities to non-military targets.

~~(S-CCO)~~ With Desert Shield/Desert Storm as a catalyst, these recommendations finally hit home. The Agency underwent major reorganization—so did several career fields. ***During this activity a "new" intelligence process was identified which was referred to loosely as Communications Research and Target Development (later modified to Signals Research and Target Development).*** It was hoped that this process [redacted]

Present

(U) Today, telecommunications networks are very different from those described above. Network structures are much more complex, being designed in a layered and functional manner. They are more dynamic—both through more rapid introduction of new technologies and through more flexible structures which enable the network to be much more active in reconfiguration. These networks support a wide range of modes and services, from simple voice and teletype, to multi-point video conferencing and broadband data transactions.



Helen Bauer of AT&T's Advanced Intelligent Networking division describes the state of the telecommunication industry as a revolution driven by revenue production. Money is a strong motivator, and the possibility of increased revenues is driving network administrations as never before.

P.L. 86-36

(U) The SIGINT community is undergoing equally radical change. We are wrestling with massive cultural changes—moving from a tiered, closed environment to a matrixed, open structure. We are faced with continually diminishing resources while the requirements on our system are increasing. The result is a very chaotic work environment.

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

[redacted]

Future—Starting Now

(U) The networks of the future will reflect incredible achievements of human endeavor. They will be structured in functional layers, enabling modularity and ease of evolution. The transport of information through the global network will be done transparently, allowing any mode or service to be conveyed in a seamless fashion. Networks are becoming extremely dynamic in configuration with traffic routing becoming very diverse, adapting easily to network outages, temporary massive changes in calling patterns, and time of day, week, or year. It will allow broadband applications and be characterized by user mobility. Software will be the key element in the global network, allowing rapid, iterative service development customized on a personal level. Network administrations, while being extremely competitive, will also be very cooperative, at both the national and international levels. Major international alliances such as those of MCI/BT, AT&T/KDD, or Sprint/FT/DBPT will drive the future of the telecommunications industry and diminish international network boundaries.

~~(FOUO)~~ Who knows what the Intelligence Community will look like? A prolonged military engagement seems unlikely now, but that's the sort of thing that is difficult to predict. The Aspin Commission and two congressional review groups make it impossible to provide any certain assessment of our future. It is possible that the Agency will move out of the realm of the Department of Defense, separating the generation of SIGINT product from the direct influence of the services or other consumers. Another area of uncertainty is the role, use, and implications of Open Sources (OS). ***The OS revolution, spurred by DCI pronouncements to make better use of OS, will have major impact on our future.*** At a time when there are massive budgetary pressures, there are proposals appearing that call for not just supplementary use of OS, but disbanding the Intelligence Community (IC). Some circles believe that the new world order, combined with the research capabilities available via the Internet, make the IC expensive and unnecessary. These seemingly radical views should not be underestimated in times of budgetary crisis.

[redacted]

The SRTD "Analyst"

(U) It has already been said that SRTD is a process, not a career field. What should the SRTD analysts be doing to prepare for the future discussed above?

~~(S-CCO)~~ SRTD analysts necessarily must be multi-disciplined but highly specialized; however, they can't be experts in everything. As mentioned previously, most will come from the IA career field, but many will come from other areas such as telecommunications, Signals Analysis, or Collection Management. The result is that much of the work requires original, innovative thought applied to problems in ways only teams of SIGINT professionals can perform. It requires a great deal of individual initiative, professional independence, and cooperative effort. ***In short, the greatest challenge SRTD "analysts" face is in developing their art and science as a team of experts.*** They are the experts in their field—whether ready for it or not!

~~(S-CCO)~~ [redacted] (SRTD Steering Group representative for A) encourages SRTD people to pursue education in their areas of interest. They know what they need to learn, so they should direct their efforts in the appropriate way.

~~(S-CCO)~~ SRTD, by necessity, is a task requiring several skills employed in very specific ways. Individuals need to develop a diverse set of skills: analytic competence (especially in traffic analysis); understanding the collection process; advanced research techniques; a

P.L. 86-36

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

high level of ADP capability; etc. [redacted] As [redacted] SRTD Steering Group representative for Z) points out, ***"The SRTD analyst ought to know how to make the system work for them—to get done what they know must be done."*** This requires close interaction with all SIGINT core processes. Ms. [redacted] sums this up by encouraging the SRTD analyst to learn to ask questions. The most important one: **"Where does the information come from?"**

Special thanks to [redacted] *in editing and refinement of the text.*

P.L. 86-36

KA

Computer Science in the year 2000

Reprinted from *Workforce 2000*

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

[redacted]

~~(FOUO)~~ System administrators will be needed to support the analysts and the networks to which they are connected. Additional System Administration personnel are required in virtually every area of the Agency, encompassing each directorate, support staff, and field sites. A System Administration Cross Training program is in place within the Computer Science Career Panel to provide a source of qualified administrators through a structured training and performance program.

~~(FOUO)~~ By the year 2000, automation and operations consolidation will result in the need for less computer operators, computer operations specialists and data flow managers. Computer Operations and Dataflow Management will be encouraged to cross-train from these career fields into others. Further, those who work in the computer operations center of the future must be multi-skilled with expertise in computer systems operations, networking, and data flow.

~~(S)~~ Computer skills will continue to be increasingly necessary for most NSA jobs leading to dual professionalizations. Computer Science/Mathematics, Computer Science/Cryptanalysis, and Computer Science/Intelligence Analysis are some of the combinations that will support our future missions.

The Telecommunications Professional Of The Future

by [redacted] former Technical Director for Q

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

(U) When plotted on a cosmic stop watch, virtually all technological advancement has occurred in the last few seconds before the present. The rate of that advancement continues to accelerate unabated. All aspects of human endeavor have been affected by this phenomenon, but none more so than the field of telecommunications.

~~(FOUO)~~ Today, every one of us is inundated with communications. We have instantaneous access to events of interest which may occur in any part of the world. It has been argued that the Western world is in a state of information overload, brought about by the incredible advances in the state of the telecommunications technology art. But what of NSA? What of its mission and the people who work the telecommunications field? A trip to an NSA communications center today would show a mix of technologies, ranging from very old legacy systems to the latest state-of-the-art. [redacted]

P.L. 86-36

(U) For each generation of technology in our telecommunications network there is also an attendant suite of skills, procedures, and processes. Consequently, our current telecommunications professionals must be adept in making a multi-generation, multi-technology communications system appear as a seamless provider of services. The demands are many. The rewards are few. It is an unfortunate historical phenomenon that the communications network is usually taken for granted by its users—until something goes wrong.

(U) NSA is not alone in having to deal with this problem. To date, industry has found it appropriate to retain much of the familiar process, and the consequent skill mix to implement it. For example, even though there have been significant advancements in the telephony and television industries, telephones and television sets still work very much as they did years ago. There are still people who climb poles, install instruments, or man switches. Advancements in transmission technology (principally fiber) and the trends toward integrating all types of telecommunications services onto the same communications infrastructure are about to change that model. The question is, "Are we ready for it?"

P.L. 86-36

[redacted]

(U) While it is technologically feasible to integrate the disparate types of services into a single network, the requisite tools for operating and managing the resultant network(s) are not yet mature. Capabilities that in the past were either not available or had to be developed by the end user himself, are now being offered as value-added services of the telecommunications system. The users are clamoring for the latest and greatest, the trade magazines try to convince the reader that they simply can't survive without the latest sophistication, and it is left to the cadre of telecommunications professionals to figure out how to make it all work together.

(U) We have made great strides in enhancing the skill mix and developing the procedures necessary to successfully cause a heterogeneous mix of equipment, tools, and technologies to function cohesively, but the task has only begun. The progress made in the telecommunications field in recent years is just the beginning, and we are on the horns of a dilemma. We cannot afford to ignore the new opportunities, but we also cannot afford to throw away the large investment in legacy systems that were designed and installed without benefit of the newest concepts for instrumentation, operations, and maintenance. Within a very short time we must be able to operate our global integrated services network from a small number of remote operations centers. Equipment must be instrumented so as to report its health, load, and other environmental information across the network to this central authority. Faults or other types of anomalies will be flagged to the attention of the network operator while the system automatically, or with operator assistance, makes the necessary routing adjustments in an attempt to assure that requisite service continues unabated.

(U) What does this mean to the work force? Certainly it will be a different world. Many skills which have served us well for so many years will no longer be necessary. The numbers and types of personnel needed will dramatically change. Our network planners must appreciate that the global network is indeed an integrated system, and plan it accordingly. We will need a cadre of more highly trained individuals to man the nerve centers of our system. A network operator of the future will need to be able to quickly assess the state of the network, diagnose trends which indicate potential failures, understand the implications of failures on the missions being served, and make real-time decisions regarding the steps necessary to assure continued service to the most critical missions. The roles of virtually every telecommunications professional, be they planners, installers, operators, or maintainers, must undergo a metamorphosis.

(U) We must help create a new generation of service providers who can synthesize from the myriad requirements the most appropriate network undercarriage, sense the pulse of the network from a central location, understand the implications of the logical missions which overlay the physical communications undercarriage, and who can engineer in real time the adjustments necessary to continue providing service. Where will we find such people? Will they come from the present cadre? Perhaps. But this new cadre will need to be educated as engineers, computer scientists, or in the fields of network analysis and computer or telecommunications engineering. They will need to be schooled in the latest network management techniques (something not readily available on many campuses). It may even be necessary for them to take the lead in shaping this particular aspect of the field. They will also need to have an appreciation of the nature and importance of the various missions which they will be supporting. Above all, they must be SERVICE-oriented.

Kλ

Global Network Intelligence and Information Warfare:

SIGINT and INFOSEC in Cyberspace

by [redacted] *Former chief, G4*

~~(S-CCO)~~ GNI (Global Network Intelligence) and IW (Information Warfare) are two acronyms that have become part of NSA's language over the past couple of years. Both convey new and comprehensive activities that are critical to NSA's future and both dramatically affect the Agency's offensive (SIGINT) and defensive (INFOSEC) missions. The purpose of this article is to provide a general overview of the background and ongoing activities in each area, to explain their interrelationships, and to discuss a few relevant challenges that are of general interest to the NSA workforce.

~~(TS-CCO)~~ GNI and IW are responses to the dramatic changes in global telecommunications that began with the transition from analog to digital communications in the 1980s. The rapid evolution of digital communications and concurrent advances in transmission media—especially fiber optics—and networking technologies have radically altered the complexion of the global telecommunications infrastructure. GNI and IW address these changes, but from different perspectives.

[redacted]

[redacted]

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

[redacted]

~~(FOUO)~~ Some examples may help to clarify the notion of a "global network" in terms of the telecommunications media involved and functions performed. When Mrs. Jones in Kansas City calls her sister in Tours, France, her telephone call is carried through the local and regional telephone network near her home, over the U.S. domestic fiber-optic network, through the undersea fiber-optic network between North America and Europe, then through the regional fiber-optic network in the U.K. and France, and finally into the local Tours telephone system. In another example, a cellular call from a Japanese businessman from his car in Tokyo to a branch office of his company in Los Angeles will traverse the Tokyo metropolitan cellular, microwave, and fiber-optic system, be routed through either the Pacific fiber-optic network or over a commercial satellite link to the U.S., then pass through the regional, metropolitan, and local fiber-optic network to the Los Angeles office. At the same time, the signalling information for this call—the 1's and 0's that provide key information to route the call and provide billing information for the telephone companies involved—may travel over a completely different path. The global network has the capacity and flexibility to provide many different pathways for connecting one user to another. As the network expands through connections of still more local, regional, and national networks, users will be able to contact other users anywhere on the globe without ever knowing exactly how their calls were completed. The same is true for data communications. This connectivity is already available for personal computer users through the Internet and for an increasing number of telephone and data services users. As technology improves, global connectivity will be faster, more diversified in terms of actual call routing, and encompass a wider variety of advanced services.

1. INFOSEC information in this and later paragraphs was derived primarily from the NSA/DI booklet, "Security Solutions for Today and Tomorrow," published in February 1994.

[redacted]

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

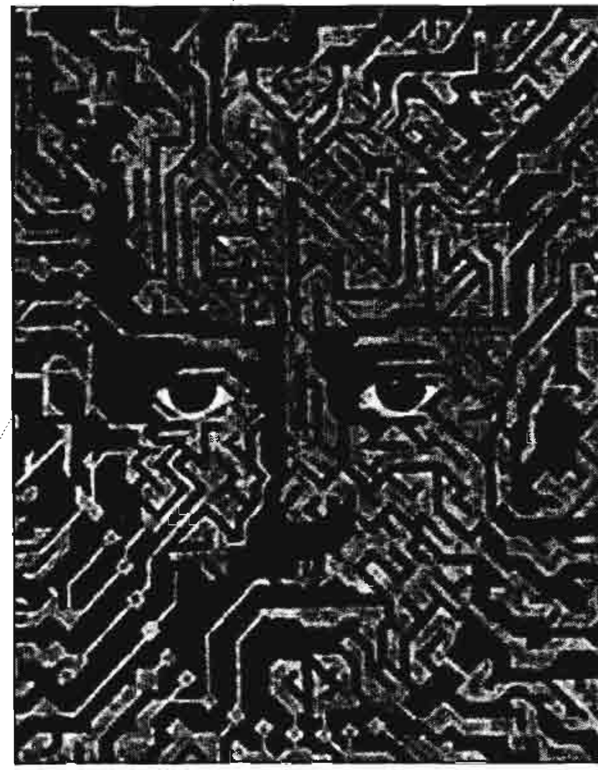
EO 1.4.(c)
P.L. 86-36

[redacted]

Information Warfare

~~(FOUO)~~ Information Warfare addresses the global network from a different perspective than GNI. IW recognizes that the rapid advances in telecommunications will directly affect the U.S. ability to wage war for U.S./Allied forces as well as for potential adversaries. Future wars may well be fought and decided on the "information battlefield" without a shot being fired. The sophisticated telecommunications and data networks now being deployed worldwide make it possible to deny and degrade a potential adversary's command and control communications and sensitive commercial and diplomatic communications from great distances with little or no risk to life and limb. Conversely, the same network technologies make it possible for a potential adversary to damage or cause confusion in communications and information systems supporting U.S. military forces or the U.S. at large.

[redacted]



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

[redacted]

[redacted]

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

P.L. 86-36

[redacted]

~~(FOUO)~~ Despite the many technical problems, in my judgment the more difficult challenges of the telecommunications revolution are in the organizational/cultural area. NSA has historically risen to technical challenges of SIGINT and INFOSEC by relying on the extraordinary talent and resourcefulness of the NSA workforce. Complex and creative solutions that would be considered science fiction by the general population are routine tools in NSA's approach to signals collection, processing, and forwarding, and information security. One should not take for granted that NSA professionals will be able to meet any and all future technology challenges, but we certainly have a good track record.

~~(FOUO)~~ More worrisome than the technology issues are the challenges posed to NSA as an institution, by which I mean the organizational culture and traditional ways of doing business. The Agency's organizational culture has changed dramatically over the past several years because of continuing budget reductions and the detailed examination of national priorities that has taken place since the demise of the Soviet Union. But as an institution we still tend to function too much as a collection of "stovepipes" in the development of new capabilities. Let me then conclude this essay with a brief description of the organizational/cultural challenges posed by GNI and IW.

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

[redacted]

Cross-organizational Communications

(~~FOUO~~) Communications among and between NSA organizations is critical. To really achieve teamwork at NSA, individual developers, analysts, mathematicians, and other specialists have to maintain an awareness of what others are doing, and, conversely, must share knowledge of their work with others. This will allow greater cross-organizational communications about various aspects of a large problem and lead to faster, more complete solutions. We need to do a better job of communicating what is going on across the Agency so that those charged with developing new GNI or IW capabilities can keep abreast of all relevant activities. Communications with external partners is another essential ingredient for future success. Such communications are vastly improved now compared to the past, but GNI and IW impose new and slightly different demands.

(~~FOUO~~) There is an expanded need for cross-organizational communications internal to NSA, too. While there is some overlap between organizations working on GNI with those working on IW, this overlap is not total. There is a continuing need for managers and technical leaders to ensure they maintain awareness of what others are doing and communicate to other organizations the projects and activities underway in their own organization. This way, cross-fertilization of ideas can take place that will help both the GNI and IW efforts.

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

[redacted]

[redacted]

[redacted]

Kλ

P.L. 86-36

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; articles 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

(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 send a soft copy via e-mail to [redacted] **cryplog@p.nsa** P.L. 86-36

Guidance

For maximum efficiency (as far as possible within the limits of your word processor):

- Do not type your article in capital letters.
- Classify all paragraphs.
- Label all diskettes, identifying hardware (operating system: DOS, UNIX), density and type of word processor used ; also your name, organization, building and phone number.
- 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**.