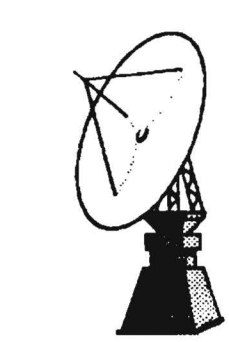
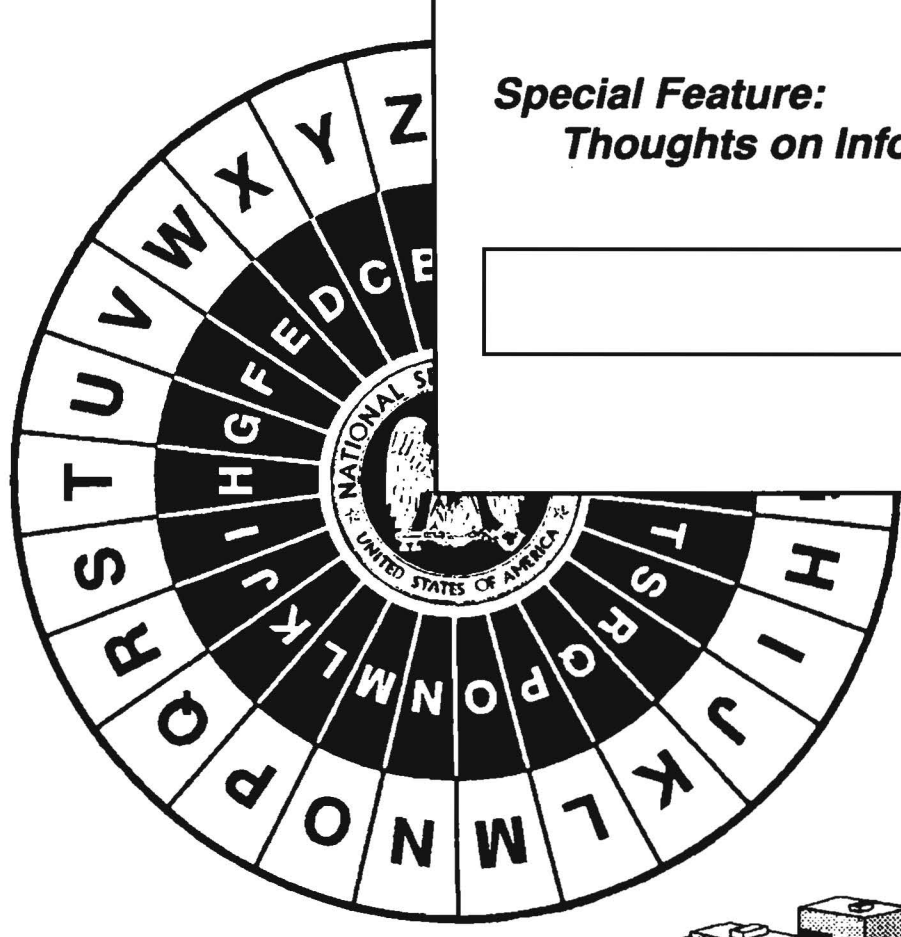
NATIONAL SECURITY AGENCY

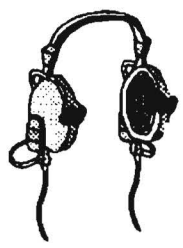
CRYPTOLOG

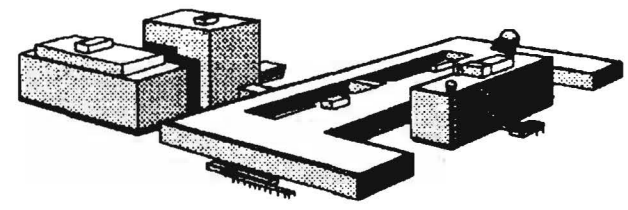
The Journal of Technical Health

Vol. XXII, No. 2 SUMMER 1996









Inside This Issue:

P.L. 86-

~~Derived From: NSA/CSSM 123-2~~
~~Dated 3 September 1991~~
~~Declassify On: Source Marked "OADR"~~
~~Date of source: 3 Sep 91~~

CRYPTOLOG

Summer 1996
Vol. XXII, No. 2

Published by P05, Operations Directorate Intelligence Staff

Board of Advisors

To submit articles and letters, please see last page.

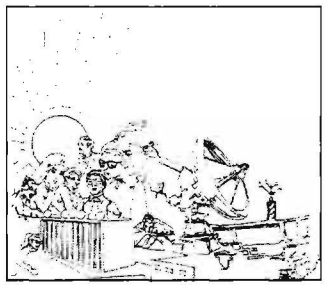


Table of Contents

P.L. 86-36

Perspective:

Confronting the Intelligence Future (U)

An Interview with William P. Crowell, NSA's Deputy Director (U)

by [redacted]
P.L. 86-36

(U) Let's start with some background: how you got into intelligence and your career at NSA.

(U) I was recruited out of college, which makes me like the majority of the professionals at NSA. It was something of a personal thing. I was so intrigued by the test NSA offered, I said to myself "Any organization that can create a test like that must be an interesting place to work." And so I decided to have the interview. I've never been disappointed, at least not for very long.

(U) And you have worked in private industry?

(U) I left here and went to a high-tech corporation, working in four areas: imagery (that's where I got my chance to learn the imagery field); low observables; mathematics research; and command-and-control systems. I started a business line that broadened their intelligence interests beyond imagery into other areas, including signals intelligence.

(U) But you're not, at least in formal terms, what one would consider a technical person.

(U) No one believes you ever have a life before you come to work at NSA. But I did have a life before I came to work at NSA. I worked for a communications company that had two major lines of work. One was designing and developing commercial communications—radio communications systems, and multi-user systems. And the second thing they did was they built [spy systems].

(U) I think the thing that's missed about my background is that I used my prior technical experience to my advantage while at NSA. In particular, more than anything, I wanted to do computer work, so in almost every assignment I've had here I was the person bringing in information technology or expanding the use of technology. I've been writing software since the early 1970s in a range of fields, including signals analysis and others, and I've never lost that interest. I still spend ten or fifteen hours every week maintaining my programming skills.

(U) Everyone was so quick to predict that the post-1945 period would be the "atomic age," but missed the coming significance of the computer, which, one can argue, has proven a far more influential technology.

(U) I had a conversation recently with the head of one of the largest of the computer corporations, and it was not until the 1950s that we began to develop a viable commercial computer industry. They had grudgingly and reluctantly modified some of their equipment so we could do computing at NSA.

(U) Can you identify two or three areas of greatest concern—make-it-or-break-it issues—as you look to the future of the Community?

(U) Let's center in on information systems and their impact on the two missions of this agency, protecting U.S. information systems and exploiting foreign information systems. One of the biggest challenges we face is balancing the two, particularly since what we do in the Defense Department and in other areas of the US government can influence the commercial market place. The systems or techniques that we develop have the capacity to come back on us in the form of increasingly sophisticated target systems. So that's one challenge I think is more than a little significant. How to draw a policy to balance those two issues is extremely important to our continued success—on both sides.

(U) The second issue is that information systems are becoming increasingly complex. For example, most communications engineers believe that it's a lot easier to ensure an error-free transmission over modern networks if there is an equal number of 0s and 1s in the communication string. And therefore they almost all—after taking lots and lots of channels, and packing them together in time or frequency, and compressing and otherwise

manipulating everything in ways that are very complex and hard to undo—add randomization in order to get an equal distribution of 0s and 1s. And randomization looks very much like encryption unless you know the way it was randomized. So, it's the complexity of all the different layers of modern information systems—whether it's the information layer, the compression layer, or the signal technology layer, or the randomization layer—that together present a real challenge to the SIGINTer. What you're saying is "undo all of this," and it's exceedingly difficult.

~~(C)~~ Let me add to all of that the third biggest challenge facing us, and that is volume. And I could just end the sentence there and everything is said.

That gives you some idea of the daunting challenge volume presents, forcing us to look for new technologies.

(U) **You don't have to go too far into the public literature to find people saying "volume wins," that the challenge to NSA and its counterparts around the world is going to be overwhelming.**

(C) Volume will never win, the reason being that volume is not the only way the world is constructed.

(U) If you don't believe that, go surfing the Web, with something you absolutely want to find, with no Web Search tools. You'll find out why someone developed Web Search tools.

(U) **One can probably find predictions of the impossibility of codebreaking going back into the 1920s.**

(U) In the 1950s, when microwave and other point-to-point communications systems were being developed, it was absolutely said that NSA would go out of business. But as a result of those communications systems, more modern means of collection were invented. When satellite communications came along in the 1960s, we developed ways of sorting through the enormous volumes of communications: dishes on the ground capable of intercepting those signals, and so on. So, in my view, virtually every communications system that has appeared on the scene, while presenting challenges, at the same time offers extremely exciting possibilities.

(U) **Do these challenges require different relationships within the Intelligence Community?**

~~(C)~~ The new information systems do not allow NSA to conduct its mission from a great distance from the target and in a totally passive manner. Therefore, the partnerships we have, let's say first with the military services, because of the need to mix tactical access with national capabilities, must become closer.

This is absolutely essential, absolutely essential. There's no backing away from that, no matter how the supporting bureaucracies may feel about it.

(U) **Do you occasionally feel resistance?**

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

(U) I've spent the last five years trying to tamp down that resistance, with some limited success. But I'm more persistent than they are.

(U) **But the argument would be, to give it its due, that we have to put extraordinary emphasis on protection of our information, and this of necessity limits how we share and how much we share.**

(U) I think that's an outmoded way of thinking. It's outmoded for several reasons. First, the partnerships I mentioned are essential. You can't succeed without them. And if you can't find a way to share the information essential to the partnership, then you ought to be prepared to sign up to go out of business. Second, the successes you may be trying to protect—the important sources and methods—have always been and will always be short-lived. You may be able to extend their life somewhat by closing the circle to absolute minimums, but you'll also restrict usefulness. And you'll

also restrict the opportunity to be successful the next time, when you're facing one of those inevitable changes.

(U) When you were deputy director for operations, you coined the phrase "SIGINT that counts," touching on what you were just saying. To acquire information, process it, and then hold onto it in such a way that it's not useful is not much of a public service, is it?

(U) I have two great fears for the future of the SIGINT system, and I challenge the system as much as I can to react to and mitigate my fears. The first fear is that we will collect what is easy to collect and pretend it satisfies our customers, instead of going after the hard-to-get (politically or technically) information they really need. The second fear is that we'll get the information and then go back to the old days of "tossing it over the transom," as Admiral Studeman used to say, or sending it to the customer and saying "Well, I finished my job. They got it." We need to realize that we have an obligation to make sure customers get the information, they understand it, and they use it.

(U) Pearl Harbor can be described as a cryptanalytic success but a cryptologic failure, in that the ultimatum message was read in time but the information got to the commanders several hours after the attack. That's a terrible but vivid model.

(U) It's absolutely an important message for us to have learned. The other message, one that comes later, and from other wars as well, is that we don't always know what the person at the other end needs. If we rely exclusively on our picks of what to send them, as opposed to relying on their ability to ask us questions or even go through our data bases to find what's important to them, we'll probably fail.

(U) Are you comfortable with a system in which the customer judges the success or failure of NSA?

(U) I've always been comfortable with that, as long as the customer is judging success within their area of interest. I don't think we should ask the Commerce Department to judge our ability to support military operations, nor do I think we should ask the military to judge our ability to support economic policy. But, yes, even if we didn't realize it, customers have been making those judgments and affecting our budgets all along.

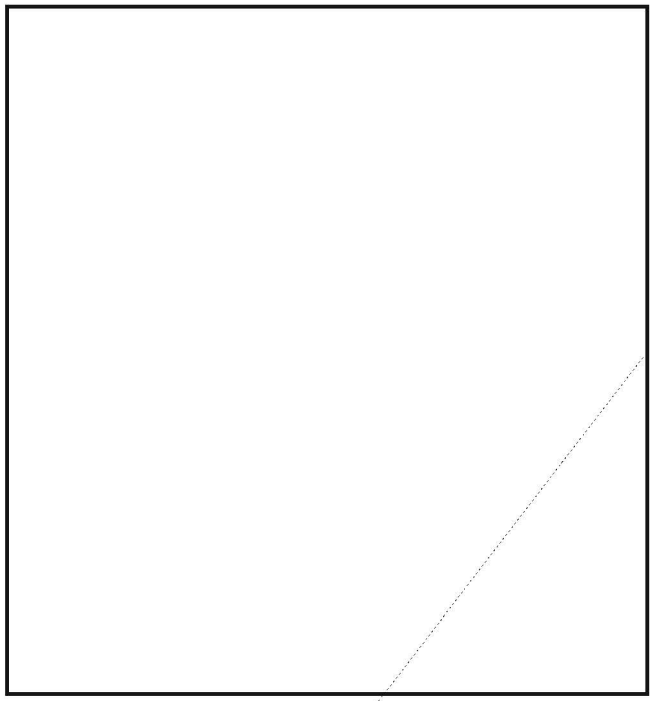
(U) More so now?

(U) But more now, particularly since the demise of the Soviet Union. With that demise came several things, the drawdown of resources, the shift of priorities, and shifts in thinking about essentiality of intelligence.

(U) Aside from the volume issue, one of the things you must hear—from the academic community, and the press, for example—is that we're experiencing a shift in the value of information. That presidents will be reacting to open-source information, on the Internet or on CNN, and that the relative value of covertly acquired information declines.

(U) I'm not particularly interested—if I may call myself a consumer of intelligence, and I think I am—in things that have already happened. I'm interested in two sets of things: those that will affect my future choices. And those aren't all going to come from open source. Second, I'm interested in those things that haven't happened yet because they're in planning. I don't think all the important information about critical, developing events are going to appear in the open.

(U) I also think one of the things we try to do too often is to pit one information source or one intelligence source against another, as if it would be possible for us to "pick a winner," and do away with all the other sources.



(U) Has the Community been successful in making the case, before Congress, among others, that we have provided information of value commensurate

~~SECRET~~

with our costs?

(U) I think that at this moment NSA and the community in general have strong stock with Congress. But there are areas of weakness we need to shore up. These range from [redacted] to our ability to cooperate.

P.L. 86-36

(U) DCI Deutch has reaffirmed his support for a policy of openness. How have we been doing with that?

(U) Recently, we've done better. Obviously, the VENONA releases were quite significant moving in the direction of recognizing when a story can be told. And that's essential. We're not going to become irresponsible. But we are going to become more responsible for being positive in our ability to recognize when stories can be released. What is often forgotten when we talk about protecting sources and methods is why we're charged to do that. Having spent the public's money to develop certain capabilities, the public expects us to maintain those capabilities as viable, as long as we possibly can, and to release those capabilities only when they no longer serve an intelligence purpose. That's an economic issue, but we often turn it into a passionate issue of different proportions.

(U) Not only do we have to change that attitude, because of the recent executive order on declassification, but, and this is a very strongly held personal position, we owe it to the American people to contribute to history what the intelligence community has done, once sources and methods are no longer an issue.

(U) VENONA is a classic example of how we can tell the story and convince the public that intelligence, at least historically, had an impact on the direction of the country. The direction of the world, for that matter.

(U) On VENONA, there was a cost to the U.S. of retaining that information, in that many Americans grew up believing there was no Soviet spy effort.

(U) As you know, I was involved with VENONA twenty or twenty-five years ago. It was one story I believed would have to be told one day. It will never end the debate, but now it's in the hands of the historians to make the judgment, not us.

(U) Let's talk about the creation of a national imagery agency. What can NSA provide in the way of lessons learned?

(U) Both Admiral McConnell and I have tried to be extremely helpful and balanced in our presentations, discussing the realities of the SIGINT stovepipe.

~~(S-CCO)~~ The realities are we don't own everything. And of course everyone who wants to reorganize the community into a new stovepipe wants to own everything, because control makes it a lot easier to get on with things. But the real strength of NSA is technical leadership and technical direction over the many people who are engaged in SIGINT, including many whose budgets are determined outside the Consolidated Cryptologic Program, [redacted] I think the imagery problem has to be solved in a similar way. They'll need to decide what the technical issues are and who decides them. What are the resource issues and who will decide those?

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

(U) Is it fair to ask about pitfalls you've warned about?

~~(C)~~ There are some very large pitfalls, with regard to the relationship between a National Imagery Agency and the organic resources within the military services, the picture taking aircraft and so on. How do you balance the need for services dependent on those resources with national needs to ensure that there exists interoperability and compatibility between systems? That will be a very tricky area, as it has been for SIGINT for a very long time. Not yet solved!

(U) The second area we've cautioned them about is when does an image become "intelligence," as opposed to "imagery intelligence?" How do you judge when someone is doing imagery intelligence as opposed to all-source analysis? We know how tricky that one is.

(U) That raises the question of the stovepipes and the bridges across them.

(U) The term "stovepipe" is very unfortunate. What we are talking about is various sets of professional and technical expertise. And we're talking about building a system of systems, one of which is a SIGINT system that has all of the necessary ingredients of training and development and science that has to do with SIGINT. It's obviously best to put all of that into one organization where it can be nurtured. The same is true of imagery, and of HUMINT. You don't want signals intelligence officers out walking the streets collecting human intelligence. They don't have the training or the background.

(U) Where do you build the bridges of cooperation and teamwork? My view is at every level across the stovepipes, instead of trying to build them on top of the organizations. You look for teaming opportunities, whether in the collection arena, in the analysis arena. We need to share technology, we need to share information, and we need to share policies.

(U) **You want to encourage people to develop their strengths in a given field, but not to act in ignorance of other fields, correct?**

(U) Exactly. That's why the bridges have to be built at virtually every level across the stovepipes. You can't just build them on top. You can't have the DDI at CIA and the equivalents at NSA and DIA as the places where the bridges are built, because what you get is three stovepipes with a plank on top.

(U) **When you look to the future and the need for technical leadership, what are your concerns?**

[redacted]

(U) **At what point does this become damaging?**

(U) It's already beginning to have negative effects. Obviously, people coming in from colleges and universities, while not able to tackle our hardest problems, are more up to date on the latest technologies, and are able to bring whole new ways of looking at things to our problems.

(U) Back to the main question, neither NSA nor CIA will ever get people out of colleges and universities—or business, for that matter—that are sufficiently trained or seasoned in this business. We'll always have to invest in specialized training and development. In that regard, I think NSA's strength is our professionalization system, which codifies that training in very identifiable directions.

(U) **As you look at problems you've dealt with over the last four or five years, how pleased are you with the progress made in transition?**

(U) That depends on where you sit. Some people outside the intelligence business may feel we've accomplished a lot, with relatively few tools and relatively little flexibility in making resource decisions. I'm personally disappointed at how long it's taking. Most people within the agency are stunned by how quickly this is occurring and would like to see parts of the process slow down.

~~(C CCO)~~ Why am I disappointed in the pace? We are drawing down, we have ever fewer resources. It is no longer possible to push decisions off into the future without it costing a great deal in the way of a continuing resource burden. [redacted]

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

(U) **It would not be hard to find critics of those decisions.**

[redacted]

P.L. 86-36

(U) **Any last thoughts?**

(U) One of the things I'll throw in as that I had the opportunity to work at CIA in the Operations Directorate early in my career, and have spent a great deal of my time in the intervening years working closely with the DO and the Science and Technology Directorate. As a result of those experiences and based on my analysis of what we face in the future, I believe the partnership between CIA and NSA can work. It requires commitment at the top of the organizations, and buy-in at the bottom of both organizations. I don't think that's been achieved yet, but it is absolutely essential to both agencies.

Kλ

Special Feature: Information Warfare (U)

P.L. 86-36

NSA Hosts JIWTAWG Conference (U)

by [redacted]

~~(FOUO)~~ The National Security Operations Center (NSOC) and the Information Systems Security Organization (ISSO) hosted the Joint Information Warfare Threat Analysis Working Group (JIWTAWG) conference in September. NSOC and ISSO requested to host this conference to further NSA's understanding of the Information Warfare (IW) threat and the integrated role that NSA can play with the Community on this issue. [redacted] This focus marked a milestone for the working group and will serve to further the exchange of information throughout the IW Community.

~~(C)~~ Lt. Gen. Minihan gave the keynote address titled "Ensuring Information Superiority for the 21st Century." He energized the working group by challenging it to: [redacted]

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

security into one. Following DIRNSA's talk, Deputy Director for Information Systems Security Mr. Thomas McDermott addressed the working group, building upon the ideas presented by the Director and stressing that the ISSO is moving toward those goals.

P.L. 86-36

~~(FOUO)~~ Each of the Services and several civilian agencies discussed their computer incident response team's structure, mission, and specific requirements for intelligence to support their missions. Also several NSA offices discussed the current support they provide and their visions for the future. [redacted]

~~(FOUO)~~ Over 200 visitors and NSA personnel attended the conference, which was the third in a series of working group meetings [redacted]

~~(FOUO)~~ To get further information about this or upcoming conferences contact [redacted] at 963-5243s or [redacted] at 963-5609s.

Kλ

P.L. 86-36

P.L. 86-36

Information Warfare: The War of the Future (U)

by [redacted]

(U) Information Warfare poses the greatest threat to the national security of the United States. Our society today, whether it be in the defense or the public sector, is becoming more technologically dependent. The immediate need for information and information systems to make decisions, to communicate, or to simply survive as a culture has exponentially grown during the last 40 years. Reliance on these expanding information systems has increased our vulnerability as a nation and analysts in the Intelligence Community are ill-prepared to deal with this new "War of Future."

(U) Those who try to fit Information Warfare into existing terminology and concepts do not accept that IW is something new.

(U) Our political and military leaders have always relied on information to plan and fight traditional battles, but the technological-dependency from which our nation suffers has made us more vulnerable to our adversaries. The "Information Age" in which our country finds itself today has led to the belief that all future wars will be information wars, and the winner will be the nation that achieves information superiority over its adversaries. That superiority is reflected in both an offensive (attack and/or exploit) and a defensive (protect) venue. Which leads to the question of how to define Information Warfare (IW)? No one appears to have a concise, clear-cut answer, and if one were to ask 50 different people that question, 50 different definitions would be supplied. The updated draft of Department of Defense Directive 3600.1 (originally drafted in December 1992) defined IW as "actions taken to achieve information superiority by affecting adversary information, information-based processes and information systems while defending our information, information-based processes and information systems." (However, not all members of the Intelligence Community (IC) could agree on the definition, and the phrase "computer networks" is to be added.) Part of the confusion in defining IW is that people try to fit IW into existing terminology and concepts, and do not accept the fact that IW is something new. The commonly held belief that IW and command-and-control warfare (C^2W) are interchangeable is a misconception that, unfortunately, is held by a large portion of IC analysts. The definition of C^2W is divided into the disciplines of attack, exploit and protect. While C^2W is a subset of IW, its disciplines are not encompassing of IW. In order to update the concept of IW, it has been divided into the following: Information Engagement (destroy and disrupt); Information Control (corrupt, deny, and deceive); and Information Assurance (defend and protect). IW includes components such as jamming/interference, physical destruction, disinformation, deception, intelligence operations, computer intrusion, and viruses/malicious codes. What analysts sometimes fail to realize is that all information systems must be considered as targets for IW, although computer systems are the most likely target, especially in the United States, where computers run our nation's infrastructure and economy.

[redacted]

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

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

Unclassified

Unclassified

(U) The most harmful computer virus will not be the one that stops your computer, but the one that randomly changes or corrupts your data over time.

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

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

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

[redacted]

[redacted]

(U) The main point is that an IW attack can come from anywhere in the world, whether it be initiated by groups or individuals, during peace or wartime. The motivation for an attack can be based on the need for recognition, political, economic, or military gain. At this time, the IC is focusing on state-sponsored attacks or plans. However, one can not overlook the individual hacker who has been hired by a foreign government to initiate an IW attack. The Internet has also become a vast resource of knowledge with hacker bulletin boards posting the latest "how to break in" information. Non-state actors, such as terrorist groups, drug-traffickers and political dissident groups, have begun using the Internet as a source to gain worldwide sympathy, supporters and funds, as well as to pass secure communications to their counterparts around the world. Pirated software can also be acquired through connections on the Internet, including several encryption software packages.

[redacted]

[redacted]

Kλ

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

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

CRYPTOLOG
Summer 1996

Some Thoughts on Information Warfare:

A critique of *"Some Cautionary Thoughts on Information Warfare,"* an article in the Winter 1995 *Airpower Journal*

by William B. Black
Chief of IW Technology Center

one team, one mission

IW

(U) As revolutions go, so far it has been bloodless. Its battle flag waves from the pages of magazines and newspapers, and its war cry resounds in briefings and speeches. It is a revolution sparked by the digitalization of communications, and fueled by the proliferation of computers and advances in technology. It is the Information Warfare revolution. Kinder, gentler folks call it Information Dominance, Information Assurance, or Information Superiority—regardless, its strategy is the same: seek and maintain the ability to exploit, corrupt, or destroy an adversary's information systems while, at the same time, protecting the integrity of one's own. Like all revolutions, this one has noble purposes: national security and national infrastructure sanctity.

(U) "Revolutions," however, are examples of change. The authors of "Some Cautionary Thoughts On Information Warfare," an article in the Winter 1995 *Airpower Journal*, are apparently uncomfortable with any change, much less a "revolution." Military historians by trade, Messrs. DiNardo and Hughes attempt to point out the problems with the IW "fad." To do this, they examine a selection of open source publications ranging from Tofflers' *War And Anti-War* book and Newt Gingrich's speech at the National Defense University to various magazine articles in *Military Review*, *Army Focus 94*, and *Airpower Journal*. They see IW developing along two lines: a) as developments to "digitize the battlefield," improve "smart" weapons, and provide "deeper-look" intelligence; and b) as an alternative to more traditional forms of war where information can be used as a weapon. It is the latter notion that is of particular concern to the authors. The article then discusses the problems of using information as propaganda (their idea of information as a "weapon"), the difficulty of defining military operations which are non-lethal, and the complications of IW in the civil liberties arena. The authors point out that information has always been valuable to the commander, that "digitalization of the battlefield" brings the danger of data-overload, and that the capability of a high-echelon commander to directly control low-echelon activities fosters micro-management. They disagree with the notion that IW plays a significant part in the Revolution in Military Affairs (RMA) concept that is currently being discussed in the Defense Community. Finally, as an alternative to this IW "fad," the authors stress the importance of commanders having moral courage, of soldiers being well trained and motivated, and of the operation being properly planned and executed.

(U) Unfortunately, their view of IW is shallow. Their mistake is that they never bother to understand what IW is, or how and why it has come about. Explained away by noting that "there is much additional material, including the very definition of information warfare, lurking beneath the shroud of secrecy,"[1] the authors are content to point out the historical mistakes in Tofflers' *War And Anti-War*,[2] to criticize those who find philosophical support in the writing of Sun Tzu, and

1. R.L. DiNardo and Daniel J. Hughes, "Some Cautionary Thoughts on Information Warfare," Airpower Journal 9, No. 4 (Winter 1995), p. 70.
2. Alvin and Heidi Toffler, War and Anti-War, (New York; Warner Books, 1993).

to condemn technological-based options to warfare. Equally important is that they apparently have little or no knowledge of computers, computer networks, modern communications, or information systems. While the authors mention some of the key issues, e.g., the importance of information in warfare, and the use of IW as an alternative to traditional warfare, their comments and criticism of such subjects are based on their understanding of history, specifically the Civil War and World Wars I and II. Lastly, it is hard to argue with the authors' alternative to IW—moral courage, training, motivation, planning—except to say that it ignores the advances in and application of information technology to warfare—advances and applications that will surely continue well into the next decade.

(S) NSA's ultimate success depends largely upon how quickly and completely SIGINT and INFOSEC merge into one in order to handle the information technology explosion of the 21st Century.

~~(S)~~ In the next decade, the requirements of NSA's customers will be largely the same: high-quality, timely intelligence information and high-security cryptographic products and services. The difference, however, will be that the environment which provides the intelligence information and the environment which is protected will be almost identical. NSA's ultimate success at meeting its customers' needs depends largely upon how quickly and completely today's separate missions converge into one in order to handle the information technology explosion of the 21st Century.

Kλ

CRYPTOLOG
Summer 1996

Joint Reporting and Inter-Agency Collaboration: Moving Out of the Box (U)

by [redacted]

(U) Many forces are propelling us toward new approaches to intelligence production and reporting: oversight committees' criticism, reduced resources, increasing workload and the complexity of intelligence issues. The report of the Aspin-Brown Commission, for instance, criticizes the fact that intelligence agencies tout the virtue of a "Community" approach to intelligence but continue to function as independent systems. Many, both inside and outside the Agency, have been urging that we find new ways of doing business. A9 is preparing for the future by setting the stage for successful collaboration among intelligence producers, both within NSA and across agencies. In addition to explaining the rationale behind joint reporting efforts, this article describes some of the projects under way that are designed to improve the effectiveness of our SIGINT reporting.

Managing the Direction of Change

"A limpet has been a limpet for millions of years. It is a 'success,' but it will never compose a symphony; it is perfectly what it is and it is stuck there."
—Anonymous

(U) The reaction of much of the NSA workforce, both analysts and managers, to collaborative reporting reveals a misapprehension about the need for this effort that leads to the illusion of a dilemma: We can do more collaborative and joint reporting but this will be a drain on the resources needed for day-to-day production. This assertion is false and betrays a lack of understanding about why we need to make this change.

(U) Collaboration isn't something for which resources must be found; it is a production process which will save resources and make the best use of analytic knowledge, whether it is used for long, hard-copy reports or for short intelligence pieces (daily product). It is not going too far out on a limb to say that in the near future there will be fewer analysts and managers but the amount of work will be the same or greater (greater in any case for those remaining). Inevitably the importance and stature of analysts will grow. But more cannot be asked of fewer without serious consequences for our production. Collaborative work is a way out of this discrepancy between need and numbers. The difficulty is that we are not structured for collaboration: our offices and group structures are historical artifacts, not entities created for maximum efficiency; we do not have a working population experienced in collaborative work; and the required information technologies are not in place. Let's examine these issues a little more closely.

(U) The National Research Council studied large-scale collaborations in the scientific community and defined collaboration as a system "linking people, computer-based tools, electronic information, and facilities to support remote, distributed, intellectual teamwork." It is important to note that the NRC definition relies heavily on the presumed existence of a robust system of electronic information exchange between dispersed participants. This is because it is only recently, with the widespread use of Internet and collaborative software, that "distributed, intellectual teamwork" has become practicable. What information technologies can now give us is wide connectivity, multimedia, shared tools and shared access so that the participants can benefit from each others' knowledge, insights, data and information. But while technology can *impel* collaboration it cannot *compel* it. This leads to the second subtext of the NRC definition: that the participants are mutually predisposed to collaborate and freely share information. In other words there must exist "a communal relationship that implies social trust and synergy among participants with mutual benefit as the result." As the Intelligence Community now stands (and this applies to intra-NSA collaborations too) these necessary conditions are not

widely found. There is little sense of communal relationship, little social trust (reporting elements often view each other as competitors), and no perception of mutual benefit perhaps because there is no mechanism for rewarding collaborative behavior. A9's collaboration initiatives are designed to address the need for this "enabling culture" as well as the need for implementing technologies.

Evolving the Work Culture

(U) The greatest challenge facing any effort toward collaboration, whether it is between offices in a single agency or among agencies, is that, technology aside, the enabling culture is embryonic at best. Whether this culture can evolve along with the collaborative technologies is moot; those technologies are already far ahead of the current work culture's ability to utilize them fully.

(U) A frequently voiced concern of managers and analysts about joint reporting goes something like, "How will we get credit for a joint report?" Various means of giving credit are already available to us; for instance, multiple by-lines can be added to a report (we have found that customers greatly appreciate this). To allay these and other fears, we can use the successful collaborations in the scientific community as a model. The NRC points out that "from a societal perspective, science advances through extensive, timely sharing of data"—and, we would add, sharing of ***knowledge*** as well—"but to advance as individuals, scientists must use their own data to the fullest extent possible before sharing them with others. Given such constraints, it can be difficult for scientists to openly share data in recognition of communal interest." The same situation exists in our agency among our analysts. To solve these problems, the large-scale scientific collaborations developed a well-defined set of "rules of the road" for their collaborations.

~~(TS-CCO)~~ Drafting guidelines to facilitate consolidated reporting within A9 is one of the goals of the EU Consolidated Reporting Advisory Team (EUCRAT), which is composed of analysts from throughout A9. The EUCRAT members have come to realize that, to be most effective, analysts need better communications, flexibility, and trust. They have only just begun translating these concepts into guidance and tools that line analysts can use. A905 has also experimented with different ways of doing joint reporting, organizing two

(U) The management of this sort of work will be profoundly different from the production process with which managers are familiar. It is essential that managers and analysts be assured that they are not embarking on some management fad, or signing on to a process that lacks leadership and support. We are fortunate in A9 that our management has given sufficient freedom of action to line managers and analysts to pursue novel working relationships and to take risks in the interest of improving the workflow.

Starter Information Technologies

(U) The absence of a completely supportive culture means that the collaborative information technologies cannot be implemented in whole, but must be supplied in functional pieces to assist analysts and managers make the change to a collaborative environment. It is essential that we run pilot studies of collaboration and joint reporting among analysts; this is the only way we will learn how to build the tools analysts need (as opposed to what computer professionals think analysts need) and it is the only way to learn the management of collaborative efforts.

It is essential that managers and analysts be assured that they are *not* embarking upon some new management fad, or signing on to a process that lacks leadership and support.

~~(S-CCO)~~ One of the first information technology tools we would like to implement, and one which will make the management of collaborative production easier, is to develop an interactive bulletin board for analytic production. This idea has been suggested repeatedly by many, including the EUCRAT as well as those who are making it possible for A933 and W9F7 to work together on energy issues. It is based on a simple premise: In order to collaborate, analysts must first know who is doing what and with what information. It has been suggested that analysts maintain a list of current and planned production as part of the NSA intranet. Analysts would consult this tool daily, and add their intentions to it as needed. Greater awareness among analysts of what is being produced by whom can only have a salutary effect on production efficiency. Redundancy in reporting (and in release and dissemination) can be avoided. This bulletin board would have an

effect on the work culture, as it would help analysts to start thinking beyond the immediate scope of their task, and get them used to working in a networked environment.

(U) A second collaborative technology we hope to implement in pilot form is a shared work space that allows co-editing of a report. To have true collaborative production, analysts must have the ability to interact freely in the production process. Some collaborative software tools available now will allow this co-editing.

(U) These attempts to affect minimum work culture and technology needs are a first cut at building intelligence production collaboration. Further steps could follow only after evaluating the results of the pilots and then introducing changes from lessons learned. This iterative process is necessary because so much is unknown. Wholesale application of a given collaborative technology on a workforce and management that is unprepared would be very disruptive. And, like as not, the tool selected would lack crucial features.

(U) It is important to remember that collaboration is not a project; it is a way of life. Individual analysts can and should begin to reach out to colleagues, without waiting for the results of formal collaborative efforts. NSA management has embraced a commitment to reward teamwork and initiative. The NSA of the future will be developed by today's innovators—our analysts and line managers.

P.L. 86-36

~~(S-CCO)~~ [redacted] *is on the Intelligence and Reporting staff of A9, the Office of Europe, Central Asia and Multinational Issues. His long-standing interest in collaboration led him into a series of efforts to promote collaboration within A9, between NSA offices, and between agencies. He has worked as an analyst in the*

[redacted]

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

research. Mike claims to have had nothing to do with the death of any of these targets. He also served as an integrated intelligence officer at the DCI's Nonproliferation Center at CIA, where he was project manager for an inter-agency collaborative reporting effort. Mike is a working microbiologist in charge of the Microbiology Dept. for a clinical laboratory in Pikesville. He spends his free time carving Mt. Rushmore on a grain of rice.

~~(FOUO)~~ [redacted] *received her Ph.D. in Linguistics last May from Georgetown University; her article in CRYPTOLOG Vol. XXI, No. 3 (*Foreign Language Testing at NSA: Time For A Change*) was based on her dissertation. She joined the Agency in 1988 as a French language intern and is certified as a language analyst in French and Spanish. At the end of her NSA fellowship in August 1995, she was assigned to the A9 Intelligence and Reporting Staff. She is currently the Chief of the B Group Language Technology Center (B638).*

P.L. 86-36

An OPENROAD to Research ~~(FOUO)~~

by [redacted] ~~(FOUO)~~

~~(FOUO)~~ OPENROAD is an initiative [redacted] to research and develop methods to simultaneously access multiple heterogeneous databases using a single query. [redacted]

~~(FOUO)~~ [redacted] to research methods and procedures to develop domain data models. We will use these models as the basis for a domain *metacatalog* (a catalog of "terms about terms") from which a user will select terms to build an OPENROAD query. Each term in the metacatalog is referred to as a *metaterm*.

The Metacatalog (U)

~~(FOUO)~~ The metacatalog is the heart of OPENROAD and is the mechanism by which an analyst can perform single-query access to multiple databases and sources. It is the link between the logical data model and the physical collection of databases, tables, fields and files that contains the data of interest. The power of a metacatalog is tthe analyst no longer needs to know the source of the data and mechanics of accessing that data. In addition, the underlying logical-to-physical mapping can change for any metaterm without affecting an analyst's ability to use that term in queries.

~~(FOUO)~~ Of paramount concern to the OPENROAD developers—both software and metacatalog—is to maintain the transparency of the data sources as viewed by the user through the metaterms. The solution we are presenting does not make a distinction between metaterms mapped to structured sources and metaterms mapped to text sources *as presented to the user,* nor does it require two queries to accomplish the same thing, one for structured data access and another for text data access. Instead, an analyst sees a logical model of metaterms from his domain, issues his query, and gets results.

The Analyst's Work Model (U)

(U) Typically, an analyst works with separate tools to gather data from multiple disparate data sources. Each tool has its own user interface and command/query language. An analyst also usually needs to remember a separate log-on and password to access each tool, database, and system. There is often little or no ability to correlate any query results or perform follow-on processing across multiple tools and sources.

~~(FOUO)~~ The focus of the OPENROAD metacatalog development is data-centric vice tool-centric. The modeling effort needed to build a metacatalog is based on the relationships among data items and how data items are used and represented, not on the tools and methods an analyst uses to get the data. The analyst has greater power to do analysis, spending less time doing the manual chores of performing access with multiple tools and interfaces. OPENROAD provides a single interface with a single log-on to all the data sources an analyst currently uses, leaving more time to do analysis.

Domains (U)

[redacted]

(U) Each information domain will have its own metacatalog tailored to its database domain. We expect

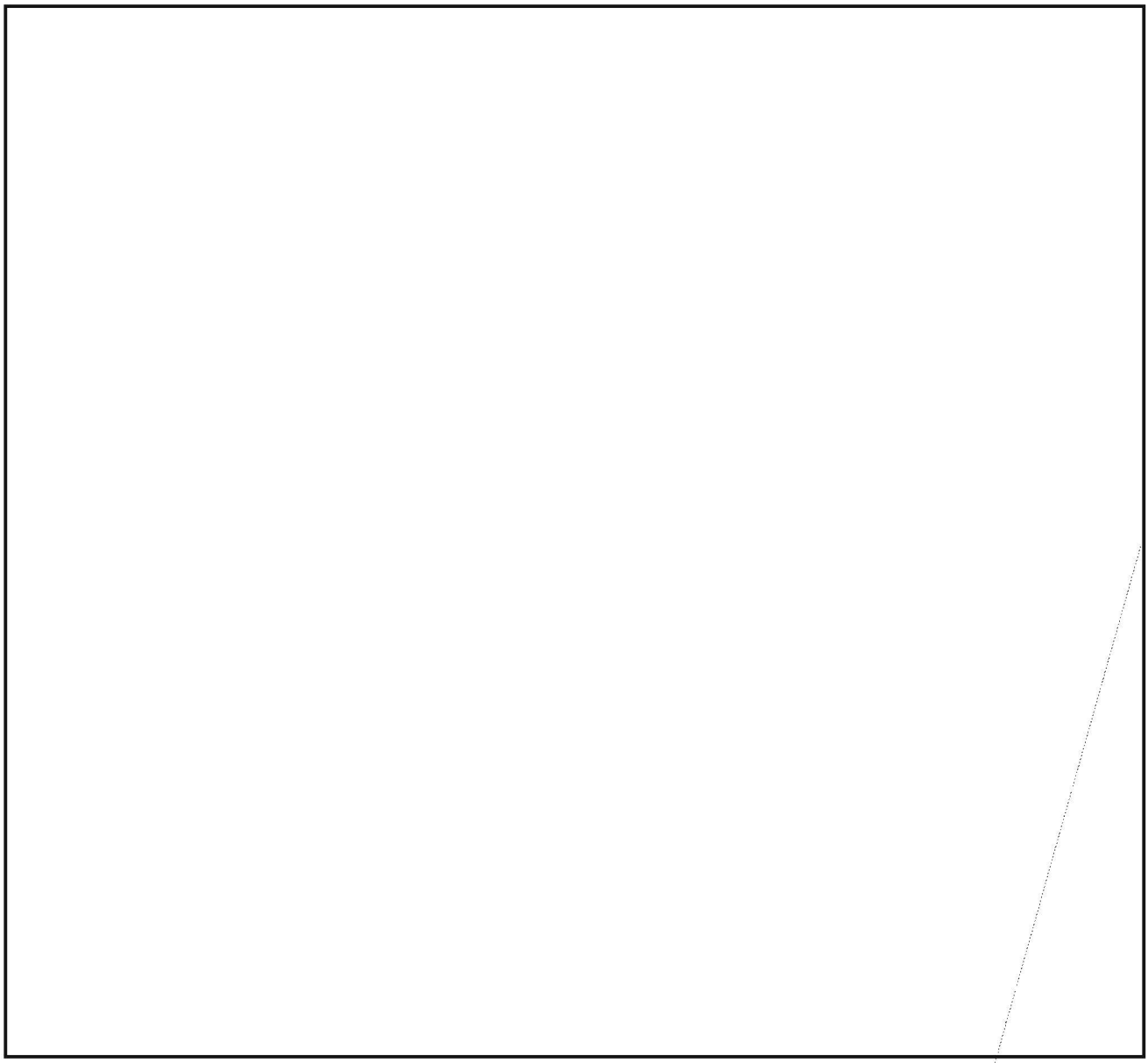
EO 1.4.(c)
P.L. 86-36

a significant degree of metacatalog reuse with other information domains that share database domains.

(U) We are currently assisting teams of domain experts (both information and database), analysts and systems support personnel in each of the prototype organizations to develop a metacatalog for that information domain. It is our long-term strategy to have domain experts and systems support personnel maintain and enhance the metacatalog once one is developed for an organization.

Key Abstractions (U)

P.L. 86-36



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

which may or may not be in hard-copy. Clearly, all these abstractions have characteristics that make one "thing" different from another "thing."

(U) Once we have identified key abstractions, we can begin to flesh them out by modeling the attributes, properties, or characteristics of the abstractions. Some attributes may, in turn, be composites of other attributes. In Figure 2, the Position attribute of a Maneuver can be broken down into Latitude and Longitude. We can then reuse Position in any new abstraction that requires geo-positional information.

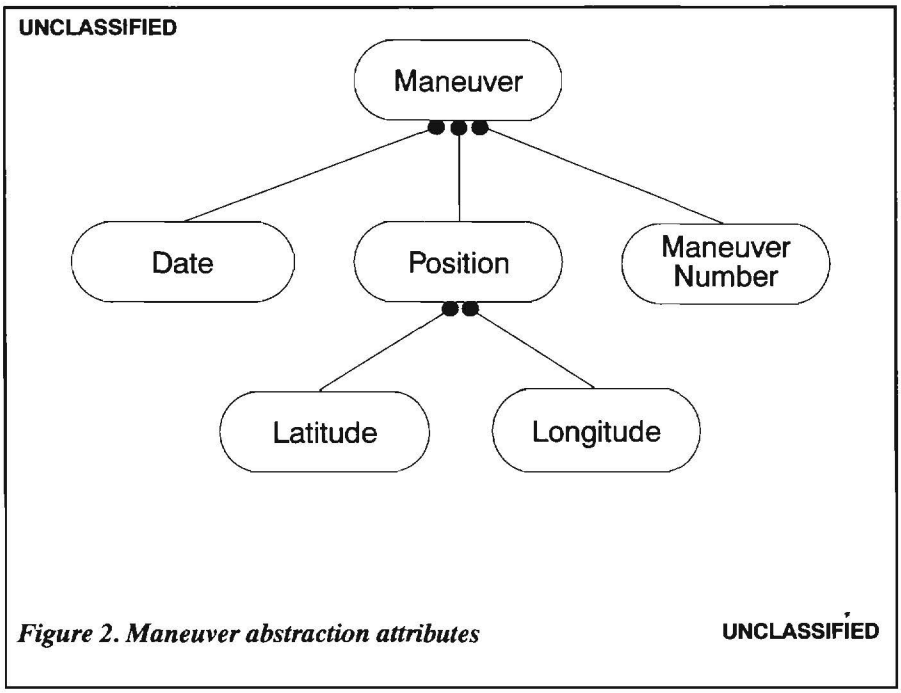


Figure 2. Maneuver abstraction attributes

Metaterms (U)

~~(FOUO)~~ When the abstractions have sufficient detail, we can begin to list the candidate metaterms from the model. Metaterms are the basic level of abstraction that an OPENROAD user sees of the information domain contained in the database domain. *Through analysis and modeling, we can create multiple "views" of the information domain.* The usefulness of OPENROAD—and of an analyst's ability to get the necessary data to satisfy requirements—is directly related to the completeness and flexibility of the metacatalog.

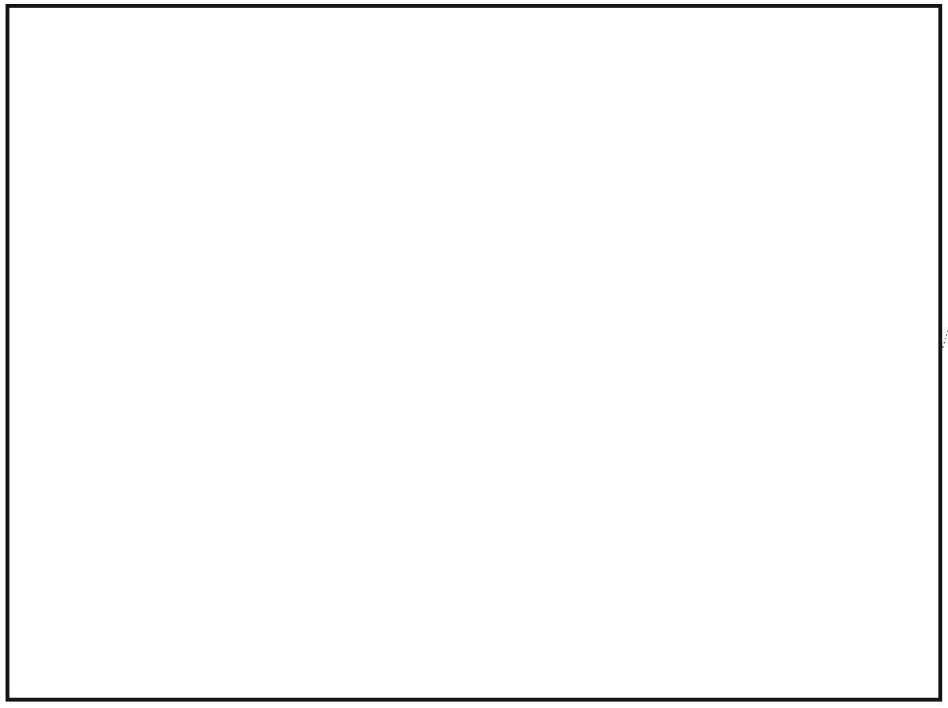
[redacted]

P.L. 86-36

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

The Logical-to-Physical Connection (U)

(S) The metacatalog provides the link between the logical domain model and the physical structure of a database. Metaterms can map to one or more fields that are semantically equivalent in one or more data sources, or to an entire data source, such as a user file.

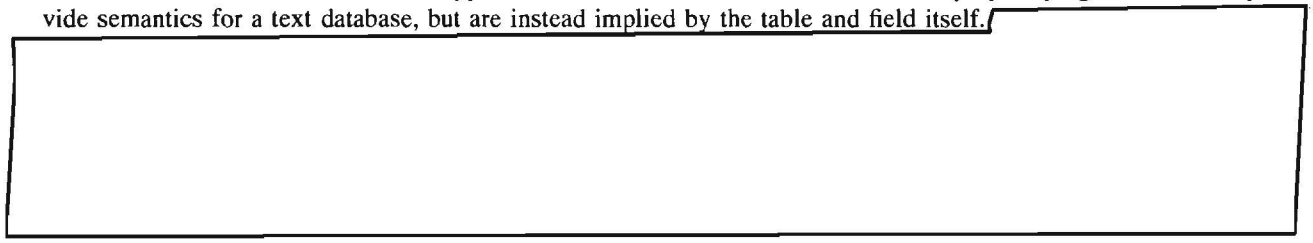


EO 1.4.(c)
P.L. 86-36

(U) One significant benefit of using metaterms is that the logical-to-physical connection can be modified without affecting the metaterm view that the user sees. If a new data source comes on-line, we can transparently (to the user) map its portion of the information domain to existing metaterms (if appropriate), or create additional metaterms.

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

(FOUO) Three types of metaterm mappings are possible. To the user, however, no distinction is made in the OPENROAD user interface. The first type of metaterm is for structured databases only; qualifying values do not provide semantics for a text database, but are instead implied by the table and field itself.



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

(U) The second type of metaterm is for text sources only. Some metaterms, like Name, may not be mapped to a field in a structured database because that source does not contain a field for names. However, this metaterm represents a valid abstraction found in the domain's text sources. A search of a text source using the qualifier "Name = 'Openroad'" would return all documents that contained occurrences of the string "Openroad", if any were found, regardless of the context in which it occurred. This type of term models data that analysts typically find only in text data sources.

(U) The final type of metaterm is for both text and structured data sources. The intent is to search for the qualifying value in both structured databases (based on semantics) and text databases or flat files (in any context).

~~(FOUO)~~ Not included in the metacatalog, but supported by OPENROAD, are free-text terms. This case satisfies a requirement to allow a search for any qualifying value for which there is no corresponding metaterm in any context in a text source or flat file.

Pangaea Virtual DB (U)

~~(FOUO)~~ The OPENROAD development team chose Virtual DB, a member of the Pangaea product line from enterWorks.com, as the tool to create and manage the domain metacatalogs. Each operational prototype will use Virtual DB.

(U) Virtual DB is itself an application, complete with a graphical user interface, for creating metacatalogs and managing access to structured databases. It runs from the GemStone object-oriented database management system from GemStone Systems, Incorporated. enterWorks.com bundles the two applications together and resells GemStone as part of Virtual DB. Since the data models we are creating are based on objects, GemStone provides great flexibility and power in storing and managing the object representations.

(U) enterWorks.com also packages Omni/SQL from Sybase with Virtual DB to provide access to heterogeneous structured databases. Omni/SQL makes the logical connections to the various databases using access modules, one for each major database implementation (e.g., Sybase, Oracle, Ingres). Virtual DB generates the necessary structured query language (SQL) statements and passes them on to Omni/SQL which, in turn, forwards the statements to the appropriate access module for each vendor's database management system. Results are passed back along the same path as the SQL statements, from the database to Omni/SQL, then to Virtual DB. Omni/SQL joins results from multiple tables from different databases and returns the results when all sub-queries are completed.

(U) Virtual DB supports pre- and post-processing data type conversions for differing internal data type representations. For example, a value representing a latitude may be stored as an integer type in one database, while in another it may be stored as a floating point type. Using a Virtual DB type conversion, we can display query results in a common format and perform Boolean operations on the data.

~~(FOUO)~~ Virtual DB can be used as a stand-alone product through its user interface. However, a rich set of application program interface (API) calls allows a custom interface, such as OPENROAD's, to access the full power of the underlying functionality directly. We currently use Virtual DB's graphical interface for development purposes. Though written in the Smalltalk object-oriented language, Virtual DB also supports a C language API. The underlying metacatalog storage mechanism is transparent to the analyst when using OPENROAD.

(U) Though not designed to access text or flat file data sources, Virtual DB does allow external data sources to be mapped to metacatalog terms. This distinction (structured vs. external source, i.e. text) is made as each metaterm is defined in the metacatalog. Each metaterm is processed according to its type.

~~(FOUO)~~ The OPENROAD team is not aware of a commercially available text gateway similar to Virtual DB for general text access. OPENROAD developers have written a custom text gateway for text source queries, using text access modules analogous to Virtual DB's structured access modules. Each text access module generates native query language for each text database (e.g. BRS or Topic); WAIS and flat-file sources are handled similarly.

~~(FOUO)~~ Virtual DB provides term-level security so each term can have its own set of classifications. Each user can see and select only those metaterms for which he is cleared. It can also enforce row-level security for mixed query results if the security labels are built into the tables of the database. Virtual DB does not, however, support security based on algorithms external to the database. Our proposed solution in such cases is to run OPENROAD at system high.

Future Initiatives (U)

~~(FOUO)~~ The DMATC will continue to evaluate other commercial-off-the-shelf products to support the OPENROAD metacatalog and to develop expertise in domain-oriented data modeling. More broadly, we will continue to research and apply methods for database access and data modeling. We intend to provide access to multi-media data sources, and allow application interoperability using the Common Object Request Broker Architecture.

(U) Our research into the process of developing domain metacatalogs is partly funded by an IDEA program grant. We anticipate additional funds to continue this research to refine and reuse the knowledge we have gained so far. We expect there to be significant levels of model reuse for many widely-used data sources.

(U) In addition, development is underway to integrate secondary queries (follow-on queries based on earlier results), text document grouping based on semantics, and filtering.

[redacted]

Kλ

P.L. 86-36

CRYPTOLOG Bloopers:

[redacted]

(U) *CRYPTOLOG* regrets the error.

P.L. 86-36

The Changing Timbre of Conflict and Conflict Resolution in Sub-Saharan Africa (U)

by [redacted] P.L. 86-36

(U) Africa has long been misunderstood. Referred to as the "Dark Continent," the "Mysterious Continent," and other inappropriate nomenclature, explorers, poets and politicians have tried for centuries to plumb the depths of this sometimes benevolent, sometimes hostile, always enigmatic behemoth. And just when it seemed like Africa's "truth" was filtering down to an audience ready to grasp its complexity, this truth began to shift once again, undermining the fledgling knowledge we all had so recently committed to memory.

(U) This shift in the foundation we had built is due to a number of factors and not merely to events inside Africa, of course. The end of the cold war changed the "usefulness" Africa held for many foreign governments—both in the U.S. and elsewhere. Africa was no longer seen as a pawn in the East/West game, its importance to politicians often generated in the past by vested national interests. To many influential decision-makers, Africa has become increasingly irrelevant within a global perspective. To a large extent, after the cold war, the world partially untethered Africa from the various links which had been artificially created and moved its focus elsewhere, leaving the enigmatic and problematic Africa more and more to its own devices.

(U) Since the end of the cold war, the world has largely left problematic Africa more and more to its own devices

(U) While the rest of the world was turning its sights to other shores or, in many instances, inward, Africa was undergoing its own evolution, struggling to find its own voice: a post-colonialism, post-cold war voice. And anyone who reads the newspaper knows about the challenges this population continues to face on a daily basis: disease, civil war, nation-building, refugees, democratization, insurgencies, outside interference in countries' internal affairs . . . the list goes on and on. In short, however, conflict in Africa has now become more regional and less global than in the days of the superpower tug-of-war.

(U) For the purposes of this article, I will concentrate primarily on Sub-Saharan Africa, leaving the study of North Africa for another time, since the circumstances of its evolution are quite a bit different for the most part. The 52 countries that make up Africa are far too diverse, their differences more glaring than their similarities, to lump together.

(U) Perhaps the most salient internal shift in Sub-Saharan Africa in the last decade has been the 1994 demise of apartheid in South Africa. Prior to 1994, South Africa was the hub of the African wheel and countries within its grasp either acquiesced to its will or fought—often unsuccessfully—to elude this grasp. Events in that part of the world seemed always to be in reaction: TO South Africa's position on a particular issue. When this relationship of inequality came to an end, at least in theory, another ripple appeared on the horizon, in the untethering most African countries were already facing. This occurred as countries in the area—particularly those contiguous to South Africa—were left to their own resources in deciding their own fate. This worked both *for* them, in some cases, and *against* them in others. It also served as an impetus for South Africa to look inward and not be as intrusive in the affairs of its neighbors. And coupled with that shift to a more defensive stance has been the burgeoning movement in both Zimbabwe and Botswana to assume greater positions of authority in the region.

(U) This new world order that was created with the demise of South Africa's apartheid and the end of the cold war has translated into new rules for co-existence among the African states and into an increasing role for the United Nations, which was paralyzed into inaction by superpower rivalries for more than 40 years. Freed from this paralysis, the UN is now being called on increasingly to help solve conflicts in Africa, to fulfill its commitment of peace-making, peace-keeping and peace enforcement there. At the same time, there has been a commitment by many of the African states to adhere to rules of non-interference in their neighbors' affairs, to maintain territorial integrity, to find African solutions to

African problems and the sovereign right to be able to ask for outside help for problems when the need arises. These rules represent significant shifts in the way that African nations do business because, until fairly recently, the sovereignty of a country could be questioned. In essence, every African was his brother's keeper and could act with impunity: South Africa was accused of interfering in the affairs of Angola, Mozambique, Swaziland, Lesotho, Namibia and other Frontline States. Zambia harbored South African freedom fighters and Liberians viewed "meddling" Nigerians as still another faction entering into the fray of their country's civil war.

(U) What African nations have discovered in many instances is that they are frequently better able to keep the peace themselves than when they ask for outside help. There are several reasons for this: one is that there is greater political acceptance of having their "own" forces present where there is conflict. A corollary to this is the expected inherent knowledge of that country's people, terrain and customs by these internal forces, the financial benefits of using "in-house" solutions for in-house problems and the superior sense of commitment that these regional forces bring to their mission.

(U) A number of events in Africa have added to the sense of confidence that many countries exhibit in handling their own issues: elections in Namibia in the late 1980's, which set up a paradigm for the entire region; peace—albeit tenuous—in Angola; the release from prison of the now President of South Africa Nelson Mandela; the end of the war in Mozambique; elections in Zambia and Malawi, and the 1994 elections in South Africa. These events and others have spurred countries on to follow suit in creating their own destinies and also in more readily cooperating with other states in the region to mitigate conflict.

(U) In a situation in which outside nations intervene in the affairs of a country, the jury is still out as to whether or not this is an effective measure. According to one camp, it is dangerous to assume that peace-keeping forces that do not respect the laws in their *own* country will be effective in ensuring that they are obeyed in *another* country. A further allegation is that these external peace-keeping forces are sometimes motivated more by financial gain than by ideological or humanitarian reasons. Forces called in to help tamp down a crisis are generally rewarded by the donor countries for their efforts with high per diems which are normally very generous, relatively speaking, with material hardware and with communications equipment. Among the more unscrupulous outside forces—these same critics maintain—the visiting forces sometimes skim off the top of the per diem to fill their own coffers.

(U) Detractors also point to the need for outside forces to lessen the appearance of partiality, to become more culturally aware of the country in which they are working, and to nurture better relations with the local population, winning their hearts and minds instead of using force. In this way, hopefully they would be better equipped to gradually earn a sense of legitimacy and a credible capacity to influence rather than to coerce. Finally, these same detractors note that there is currently no joint UN publication which outlines peace-keeping procedures and guidelines, no system of checks and balances to standardize operations. It is left up to the various coalition armies to determine on their own, with their divergent backgrounds, agendas and motivations—not exactly a recipe for success by most standards. And with the UN expected to increasingly play a major role in peace-keeping in Africa, it is incumbent upon that organization—with its 50 years of experience—to help standardize and thus legitimize its missions there.

(U) One problem with UN missions that is particular to Africa is the declining level of awareness of people *outside* Africa. An illustration of this deterioration of external knowledge is the widely-held theory that Africa is composed of hegemonic tribes and subordinate tribes with conflicting philosophies. Under the terms of this theory, every conflict in Africa can be reduced to ethnic terms, regardless of the context. One size fits all in this simplistic paradigm which, unfortunately, is gaining prominence in some quarters, irrespective of the multitude of economic, political, geographical and historical factors which have all contributed enormously to conflict in Africa. For example, four civil conflicts have been cited to corroborate this monochromatic theory: the Congo/Zaire upheaval of the 1960's, Somalia, Rwanda and Liberia. Instead of examining these four situations through the lens of an impartial, astute observer—taking into account the less-than-ideal role played by the UN in all cases—they have been reduced by some to wars between barbaric tribes of Africa, tribes with little else to do than wage war.

(U) There are those who would argue, however, that in the case of the previously mentioned conflicts and in others, a finger should be pointed at the UN, which has traditionally played a more *re*active than *pro*active role in Africa. In addition, as previously indicated, often there is a lack of a clear framework for UN operations abroad and what starts out as a particular type of mission can sometimes change in midstream,

without any apparent rationale.

(U) Still another criticism of UN peace-keeping operations is that they are, in fact, peace-*keeping* and not peace-*making* operations, that the emphasis is on the wrong aspect of operations. Allegations have been leveled against UN officials for purportedly bailing out when the "going gets tough." When the conflict escalates—these same allegations continue—the UN threatens to pull out, leaving the country in question in the lurch. Still others accuse the UN of not providing sufficient funds to its peace-keeping operations and of channeling too many funds into bureaucratic areas. Two examples cited as the worst of the UN missions to Africa are Somalia and Rwanda. Finally, the critics charge that the UN needs to address underdevelopment in these African countries or people will continue to be galvanized into fighting against a common enemy: poverty.

(U) Africa's own foreign policy reflects the changing perspective on conflict and conflict resolution. Before the end of apartheid, the Frontline States wielded considerable influence in the region, concentrating their collective efforts on dealing with a common adversary: South Africa. There had also been another common enemy to provide these African countries with a united front: colonial/European rule. With the shift in perspective that resulted in the end of apartheid and the end of colonial-ruled Africa, foreign policy there fractured into multiple, often contradictory and competing philosophies as these once-united African states scattered for divergent political shores and, in doing so, lost much of the power base they had enjoyed when they were part of a more unified whole. Without their former collective power, their leverage in a global sphere has been reduced considerably.

(U) Coupled with this fragmented foreign policy is the lack of an economic power base to recreate some sort of linkage between these countries. African states were so preoccupied in their respective post-colonial periods with nation-building that economic considerations often fell by the wayside.

(U) In order to remedy this situation, some advocates of South Africa's historic hegemony in the region advocate a controversial return to this type of arrangement, but with a benevolent (versus exploitative) model. Under this type of relationship, the constellation of African states would again revolve around South Africa, but a benevolent South Africa which would now act in a manner beneficial not just to its own interests but to those of its neighbors. The previous asymmetry which

Unclassified

Unclassified

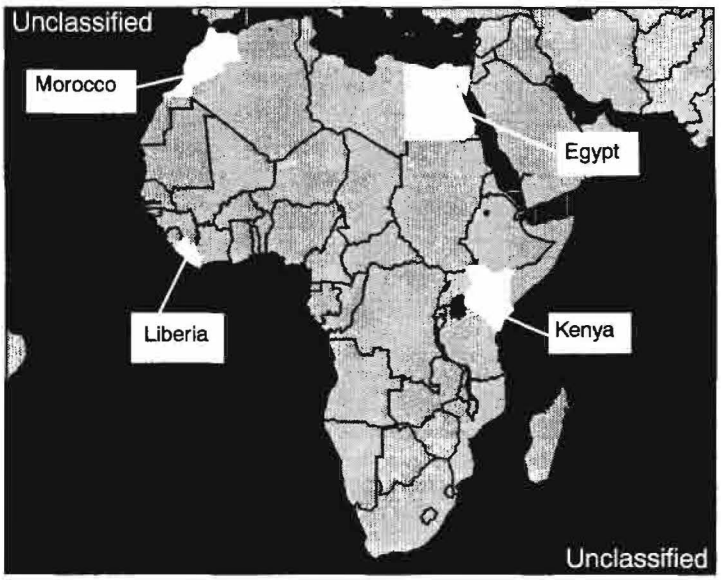
(U) Government forces face increasing challenges from insurgents and/or gangs

reigned in an apartheid South Africa would still exist but under this theory South Africa would temper this hegemony by remaining ever-cognizant of the interests of its wards. The relationship would also be more multilateral in nature, with the economic and institutional needs of each country of prime importance. Naturally, in order to be successful, it would require the willingness of all parties to cooperate.

(U) The antithesis of this benevolent model is an exploitative system, one which was the norm in South Africa for many years. This model harks back to the not-so-distant past when national interests were of paramount importance and countries related to each other on a bilateral basis for the most part, leading to regional imbalances and frequent conflict.

(U) Time will tell if the so-called benevolent model takes root in Southern Africa. In order to meet with success, South Africa's neighbors will have to want growth and stability more than they want to usurp South Africa's hegemony. And South Africa will have to prove to these same neighbors that its goals extend beyond its own boundaries to the common good of the region, and then not exclusively to its European and American counterparts.

(U) Adding to the complexity of the discussion of conflict and conflict resolution in Sub-Saharan Africa is the issue of arms transfers since the end of the cold war. The exodus of the superpowers from Africa has meant that governments there no longer enjoy the luxury of financial assistance in boosting the equipment of their security forces. Conventional military equipment is no longer so easy to come by now. Conversely, in many of these countries, automatic rifles are often cheaper than a



(U) Basing agreements in Liberia, Morocco, Egypt, and Kenya will remain key issues for the U.S., but primarily for purposes of power projection outside Africa.

loaf of bread and often as accessible because of the enormous amount of weaponry brought into Africa during the cold war and then left behind. This means that government forces are now increasingly vulnerable to challenges from insurgents and/or gangs. Furthermore, these same governments are less and less successful in engaging Western governments to assist them in their fight against these hostile forces. It is important to keep in mind, too, that African governments frequently find it difficult to ensure that material resources are distributed to the masses, therefore, the military is becoming a determining factor in ensuring their delivery. If it is under attack or vulnerable to disruptive influences, it affects the entire population of a country. When national armies are outmanned and outarmed by insurgents, political dissidents have no reason to eschew violence.

(U) With this shift in the nature of arms acquisition, conflicts in African states are now being prolonged, and are more intense and frequently more difficult to resolve. And with the decline of legitimate economic activity, force has become the lingua franca in obtaining resources and has meant that conflict often spills into other areas. Examples of this spillover include Liberia (Sierra Leone and Cote d'Ivoire), Rwanda/Burundi (Zaire and Tanzania), and Angola and Mozambique (South Africa).

(U) A corollary of this new paradigm of conflict is that there are very few outright victories in Africa and this is due, for the most part, not to the strength of the insurgents but to the relative weakness of the government in defeating these insurgents. Most African armies are not properly organized, equipped or trained and, therefore, ill-equipped to combat the well-armed insurgencies.

(U) A further impediment to conflict resolution is the fact that negotiated settlements are very difficult to achieve in Africa, for the following reasons:

- the insurgents often have no clear-cut ideology; ideologies are often personality-driven, or new players come into the picture, preventing consensus. This results in an ever-changing and therefore confusing insurgency ideology;

- factions proliferate as the conflict is prolonged. This factionalization inhibits the government's desire to settle the conflict since there is no clear-cut *single* adversary (e.g., Somalia, Angola and Liberia). As a consequence, the government often fails to recognize factions as *legitimate* factions representing the whole. This factionalism also works against achieving consensus among the many disparate parties;

- there is a lack of education in the negotiating process itself (e.g., Mozambique, Ethiopia and Rwanda);

- during the negotiation phase—if reached—few countries have the money to finance the logistical aspect of peace talks;

- there is rarely international support to sustain peace, which may delay the process (Mozambique) or lead to a breakdown of negotiations (Liberia);

- there is a shifting idea of what victory/compromise/defeat mean to the parties involved; and

- the country or countries involved have been virtually devastated.

(U) As the face of Africa changes, a sense of pessimism can be detected in some quarters. As conflicts there increase, there is a marked loss of hope, the long-standing hope that the lot of a post-colonial Africa would be better—both economically and politically.

After almost three decades the opposite is true more often than not, and the term Third World still applies to most of the continent, with the exception of a portion of South Africa's population and small pockets in other countries.

(U) The United States will always have a strategic interest in Africa and its welfare but this interest will shift as the situation both in Africa and the U.S. changes. Basing agreements in Kenya, Morocco, Liberia, and Egypt will remain key issues for the U.S. but primarily for purposes of power projection *outside* Africa, not inside Africa. In addition, oil, strategic minerals, humanitarian and relief operations and an interest in keeping sea lanes of communication open at both the Horn and the Cape of Good Hope form the basis of continued U.S. interest in Africa. Nevertheless, in an era of decreasing budgets and increasing domestic focus, it will fall more and more to Africans themselves to sort out their conflicts, to find African solutions to African problems without relying on outside help or by relying on the assistance of the United Nations.

[redacted]

P.L. 86-36

Kλ

~~(FOUO)~~

Inter-Agency Conference

"Responses to Humanitarian Crises: the Role of Classified Intelligence" co-sponsored by NSA and CIA.

The purpose of the Conference is two-fold:

1) to identify the types of classified intelligence customers need and do not need in the time leading up to, during, and in the aftermath of humanitarian crises; and

2) to identify intelligence gaps and other issues that affect intelligence producers' ability to meet customer requirements.

Date: 3 December 1996
Hours: 0815-1600 (Registration begins at 0800)
Location: 9A135, Headquarters

Credit for NCS course IS-355 (Current Issues in Intelligence Analysis) will be given for attending this conference; interested students should preregister by contacting Conference Co-Chair [redacted] on 963-6011s.

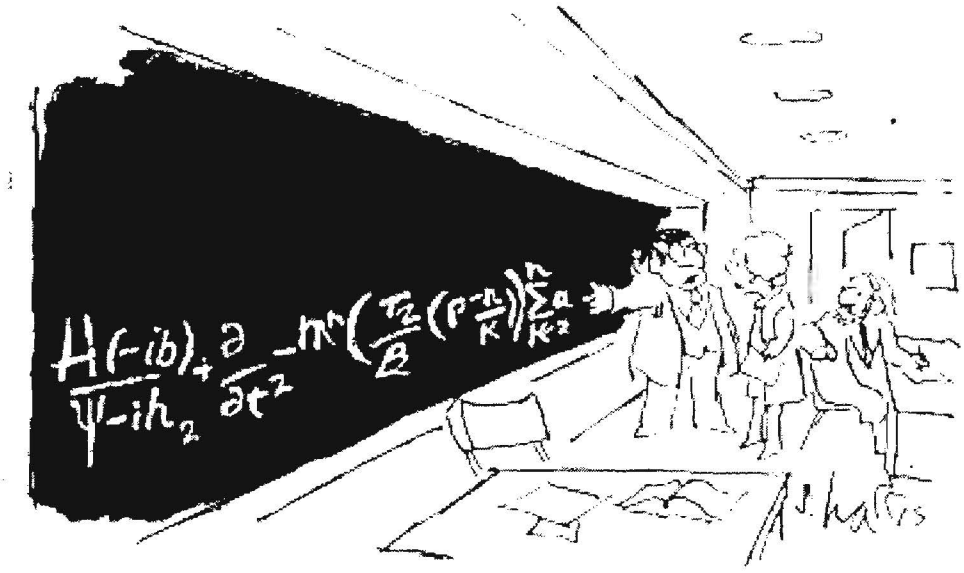
P.L. 86-36

Calling all publishers! (U)

P.L. 86-36

~~(FOUO)~~ We are looking to update an article that appeared in *CRYPTOLOG* Vol. XX, No. 2: [redacted] *Publishing as a Member of the Technical Track*. This article listed a number of Agency publications that provide the opportunity for disseminating information "as a vehicle for both technology transfer and career growth": for instance, *The DD Eye*, *Cryptologic Quarterly*, and the *Infosec Technical Exchange*. Since *CRYPTOLOG*'s focus is on explaining developments in one's field to those outside it, we would like to spread the word that since [redacted] article appeared, a number of new periodicals have appeared, and we have learned of others that existed at the time. *CRYPTOLOG* would like to add to this list of vehicles for contributing to one's skill field. To quote from the article, "Are there any journals which regularly come across your desk or to your computer screen? How about newsletters and other local publications that you've seen? Most Agency technical societies solicit papers on an annual basis for essay contests; look for the announcements or contact one of the society's officers. How about an organizational technical report that carries a wide distribution? Career Panels and Technical Directors can also help point you in the right direction." If you know of such an opportunity, please provide the *CRYPTOLOG* editor with the name of the publication, its editor, a description of its mission, and instructions for submitting articles.

Unclassified



"But this *is* the simplified version for the general public."

Unclassified

~~FOR OFFICIAL USE ONLY~~

by [redacted] P.L. 86-36

The Need for Multilevel Secure Databases (U)

(U) An information downpour is flooding the Agency. NSANET and client/server architectures have created an environment in which users can transparently access data that resides on remote systems. This situation affords many advantages, including the quick and paperless dissemination of information, but it has also become easier for information to get into the wrong hands. When computers with varying security levels reside on interconnected networks, unauthorized users may read information at a classification level higher than their own. The consequences of unrestricted data access range from the accidental retrieval of classified information by those without adequate permissions to the intentional transfer of classified data to those whose goals lie in the areas of profit and espionage. This clearly is a situation we cannot allow to exist. We must take precautions to ensure that data can be accessed only by users with adequate authorizations.

A Possible Solution: Trusted SOLARIS (U)

(U) The easiest way to protect classified data is to locate it on stand-alone machines or networks that carry data of a single security level. These machines or networks would be accessible only to authorized users. This may seem like an antiquated proposal, but this was the norm until recently. With security mechanisms such as cipher locks on doors, automatic screen lockouts, and restricted local area networks, the necessary controls were provided. Data at a single classification was placed on a machine, and only authorized users could access the machine. Users in today's environment have requirements that make this method inconvenient and overly restrictive. They need to be able to access data remotely across multiple networks and at multiple security levels. They also want to integrate information residing on different machines or networks, or transfer information to their local workstations.

~~(FOUO)~~ Many organizations investigated secure operating systems as a better means of providing data security. These operating systems are known as Compartmented Mode Workstations (CMW) and must fulfill requirements specified by the Defense Intelligence Agency. The K223 BOXOAK project decided to base its architecture upon Sun's version of CMW, the Trusted SOLARIS operating system. This product is designed to allow users at different clearances to handle information at different levels of security while protecting the security of that information and keeping it properly labeled. It accomplishes this through the use of privileges, separation of administrative roles (there is no "root" user), and labeling of users, programs, and information. Trusted SOLARIS is the backbone of the BOXOAK Phase 1 operational system used by K53, and ensures the separation of compartmented information.

~~(FOUO)~~ BOXOAK's plan was to continue using Trusted SOLARIS during later phases, with the addition of a secure relational database management system (RDBMS). SYBASE, INGRES, and ORACLE, the three major databases at the Agency, all have secure versions of their product lines that run on CMWs. A secure RDBMS would make it possible to develop software without the need for any special algorithms to guarantee data security filtering. For instance, if a user was operating at a CONFIDENTIAL clearance level and requested information from a source that included classification levels ranging from UNCLASSIFIED to TOP SECRET, the user would only be provided information at the CONFIDENTIAL level or lower. Furthermore, the fact that information existed at higher levels would not be apparent to the user.

(U) Initially, the INGRES/Enhanced Security product was used, and it performed as desired. Due to the widespread Agency use of SYBASE, the decision was eventually made to switch to the SYBASE database product line; again, data security was provided exactly as described. Although these secure RDBMSs worked well, their dependence on many features pro-

vided by the operating system was a major drawback because concerns about Trusted SOLARIS were surfacing and could not be ignored.

~~(FOUO)~~ BOXOAK had remained in regular communication with Y4, who was performing an operational test of Trusted SOLARIS for use in the DDI Virtual Campus architecture. Y4 found many flaws with the product and eventually decided not to use Trusted SOLARIS. At the same time, BOXOAK was experiencing many of the same problems Y4 was documenting. These problems were all of a fairly serious nature and had to be considered.

- (U) CMWs are not widely used, and it was impossible to find expert guidance and assistance in other organizations.

- ~~(FOUO)~~ SUN was providing only minimal support for Trusted SOLARIS. BOXOAK was dealing with one point of contact who moved to another product line. Support was virtually nonexistent after that.

- (U) Further development of Trusted SOLARIS was negligible at best. It was supposed to keep pace with the non-secure product releases, but this did not happen. As a result, many new tools could not be installed and used. This was a major problem when the Graphical User Interface (GUI) development tool that had been purchased could not be used since it required a newer release of Trusted SOLARIS than was available.

- (U)) There were reports of vulnerabilities with the very security which Trusted SOLARIS was designed to provide. CMWs are built to protect a multi-level, compartmented environment but have been found to be exploitable.

(U) These issues alone would have necessitated a hard look at the wisdom of using Trusted SOLARIS. When coupled with the fact that the secure RDBMSs were 50% more costly and much more difficult to maintain and administer than their non-secure counterparts, it was decided that other alternatives to providing the necessary security had to be found.

Alternative Solutions (U)

~~(FOUO)~~ During conversations with SYBASE, the company had alluded to a new Secure SYBASE product that would not require a underlying secure operating system. This would have met many of BOXOAK's security needs. Unfortunately, this product never became available, and still does not appear to be on the horizon. BOXOAK had to keep its investigation active.

~~(FOUO)~~ An in-house product known as SENTINEL came to the attention of the BOXOAK team. This A74 product provides SYBASE security filtering without the need for an underlying secure operating system. SENTINEL was designed initially to support other A74 applications with security filtering needs much more complex than BOXOAK's. Implementing these requirements incurs some cost in terms of maintenance and performance. SENTINEL also required the purchase of additional SYBASE software which otherwise was not needed. When it was finally determined that BOXOAK did not require as elaborate an architecture as the A74 projects, the costs seemed to far outweigh the benefits.

~~(FOUO)~~ Since there were no other security products to be found, there was only one course of action left. BOXOAK would design and develop its own simple and easily maintained data security mechanism.

The BOXOAK Solution ~~(FOUO)~~

~~(FOUO)~~ The requirements for the BOXOAK implementation were driven by the needs of the customer, the K5 High Altitude Programs, which include many Configuration Control Boards (CCBs). These CCBs operate at varying security levels and will be accessing the same BOXOAK system to manage their programs. It was required that users would only be able to access and be aware of information to which they had an equal or greater security level. Furthermore, the networks over which this data would be transferred would need the same protections.

~~(FOUO)~~ The BOXOAK solution was multi-faceted and was based upon the strategy employed by the SENTINEL product. This strategy was fundamentally sound and its use would facilitate future interfaces between the products. The implementation includes the database design, modified database queries, and a few translation algorithms; it will be used by all BOXOAK systems.

Database Design (U)

~~(FOUO)~~ Some essential terminology must first be explained. Normally a user has a clearance and data has a classification. BOXOAK, like SENTINEL, deviates from this convention. Both users and data have a **classification** which includes the national clearance (e.g., UNCLASSIFIED, SECRET), handling codes (e.g., US, UK), and compartments (e.g., TK, B). SENTINEL uses the terms **privacy** to refer to handling codes, and **special access** for compartments. For consistency's sake, BOXOAK also used the terms privacy and special access to refer to these codes.

(U) Three database tables containing all possible values for clearances, privacy codes, and compartment codes are the core of the security strategy. The table structures, including some sample data, appear after their descriptions.

(U) The clearance table contains all possible values for clearances. Since only one clearance can be assigned to an item at a time, a single integer is used to designate each clearance. This integer is the value actually associated with an item when it is stored in the database. Also stored in this table are the full and abbreviated labels for the clearance, used for displaying text on the screen or on hardcopy. A color (bgcolor) is stored and is used as the background for the classification stripe on any screen displays. A second color (fgcolor) indicates the color of the text on the classification stripe and is limited to the values of black (B) and white (W). As an example, an UNCLASSIFIED clearance would be displayed on a stripe with black text on a green background.

Clearance Table ~~(FOUO)~~

value	clearance	full clearance	bgcolor	fgcolor
0	U	UNCLASSIFIED	green	B
1	FOUO	FOR OFFICIAL USE ONLY	limegreen	B

~~(FOUO)~~ A data item could have both multiple privacy and special access codes. For instance, a TOP SECRET item could have privacy codes of UK CA and special accesses of TK VRK. As a result, these codes had to be handled differently to facilitate assigning multiple values to a data item. In both the privacy and special access tables, there is a label field which contains the actual code. There is also a position field (stored as an integer) which represents the code's position in a bitmap associated with a data item. When a data item contains a 1 in its bitmap in the designated position, it indicates that the code applies to that data item. For example, if a data item is marked with a 3 in its privacy field, the corresponding bitmap (binary equivalent) is 011. The codes that correspond to the zero and first position (starting at the right) would apply to this item. A lookup of the privacy table shows that a 1 in the rightmost or zero position indicates the US code, and a 1 in the first position indicates a UK code. The same design is utilized in the special access table, which also contains a full label field containing the full text of the code (i.e., Talent Keyhole for TK). This full label was deemed unnecessary for privacy codes.

Privacy Table ~~(FOUO)~~

label	position
US	0
UK	1
CA	2

Special Access Table ~~(C)~~

label	position	full label
SI	0	COMINT
TK	1	TALENT KEYHOLE
B	2	BYEMAN

(U) Tables with secure data contain these three integer fields corresponding to the three classification tables. Other tables that interact with this data, including users and devices (hosts, networks, printers) also contain these fields. Thus, an entry in the User table contains user information (i.e., name, SID, organization) as well as the clearance, privacy, and special access fields. The values in these three fields can then be compared to the values in the fields associated with a specified data item. Access is allowed only when the values in the data item are dominated (equal to or are exceeded) by the user's values. The mechanism for restricting this access is implemented by the retrieval criteria in database queries, which is described in the next section.

~~(FOUO)~~ A single integer field can hold up to 32 privacy or special access codes, which is more than sufficient for BOXOAK. This design can be extended to multiple integer fields if an application requires a greater number of codes. Any number of clearances can be accommodated, but since these are controlled at the national level, there is little chance they will be modified.

(U) A Colors table also exists. This table lists all possible combinations of values in the special access table and associates a color with each. If one or more special access codes exist for an item, the color from the Colors table is used in the classification stripe on screen displays and supersedes the color associated with the clearance value.

Colors Table ~~(FOUO)~~

value	label	bgcolor	fgcolor
1	SI	DarkOrange	B
2	TK	yellow	B
3	SI TK	Tomato	B

Database Queries (U)

~~(FOUO)~~ Once the data is labelled with the appropriate classification, database queries must be carefully constructed to ensure that security filtering takes place. In the case of the clearance field, the requirement is met by checking that the user has a clearance level that dominates the requested data. Only data that meets this criteria is retrieved. For the privacy and special access fields, security filtering does not equate to domination. The user must possess all codes assigned to the data item before it will be retrieved. If a data item has a privacy code that maps to US, UK and CA, then the user must have at a minimum all three of these privacy codes. Logical bitwise manipulations are used to provide this assurance. The data value is logically ANDed with that of the user and, once again, only the correct data will be retrieved. An example of a query with the correct criteria follows:

```
select B.board_name

from Boards B, Users U

where  U.username = 'jones' and

B.clearance <= U.clearance and

(B.privacy & U.privacy) = B.privacy and

(B.special_access & U.special_access) = B.special_access
```

~~(FOUO)~~ The results of this query are based on the data in the following tables (bitmaps and sample compartments appearing in parentheses for illustrative purposes only). User "jones" lacks the SI special access code and will not even know that a NW CCB exists. The user's clearance dominates the BOX CCB's clearance, and all of the BOX CCB privacy codes are contained within the user's privacy codes. The BOX CCB will be retrieved.

Boards Table ~~(FOUO)~~

board_name	clearance	privacy	special_access
BOX CCB	3	5 (101)(US CA)	4 (100)(B)
NW CCB	4	2 (010)(UK)	3 (011)(SI TK)

Users Table ~~(FOUO)~~

username	clearance	privacy	special_access
jones	4	7 (111)(US UK CA)	6 (110)(B TK)

Translation Algorithms (U)

~~(FOUO)~~ Classifications are always displayed to BOXOAK users as text since they have no knowledge of their underlying integer representations. There was an obvious need for a suite of algorithms that would provide the translation from text to integer and from integer to text. Four functions were developed to satisfy this requirement. Two functions support the translation of the clearance, and the other two translate both the privacy and special-access codes. These functions were written in embedded C/SQL so that they could be easily ported to other RDBMSs should there ever be a need. A final function was written to assign colors for classification text. These colors were used to determine the background color for the classification stripe on windows as well as the color of the classification text itself.

Network Considerations (U)

~~(FOUO)~~ BOXOAK systems will communicate with one another across Agency networks. Each system will have both a high and low classification associated with it, defining the full range of information residing there. The network across which these systems will communicate will also have a maximum classification associated with it. These levels will be available to the software to ensure that data cannot be transmitted to a system with an insufficient security level. Encryption is also available to provide security for data transmitted over networks and is employed by BOXOAK. Even when network levels allow the flow of classified information, the classifications of the receiving system and user ultimately decide whether the data transfer will take place.

~~(FOUO)~~ Another threat must be considered. While BOXOAK ensures that data is available only to authorized users, the SYBASE RDBMS can be directly accessed outside the application through the Interactive SQL (ISQL) command. Most BOXOAK users will not be granted the UNIX shell from which this ISQL command is executed; some administrative users will have shell access. The use of the SYBASE OpenClient software also makes it possible for a determined user to access these databases remotely. The ISQL access problem can be handled in a few ways. For instance, a wrapper performing access control can be written around the command to prevent its direct execution. Permissions on this command can be set to include a very limited group, excluding the general user community and eliminating the possibility of back-end access.

Advantages (U)

(U) It is usually preferable to use commercial products to provide system functionality whenever possible. The reasons stated earlier pleaded the case for development of a home-grown tool that meets the fundamental requirements of separation of multi-level information and prevention of unauthorized access. Other significant advantages were found as a bonus. These include:

- **Low Cost.** This strategy is significantly cheaper than the alternative of buying both a secure operating system and RDBMS. Developing the algorithms involves some resources, but these are reusable.

- **Simplicity.** The mechanisms for providing security are easily described and documented. They consist of a few additional classification tables and fields, modifications to queries, and a handful of translation algorithms.

- **Ease of Administration.** A standard operating system and RDBMS are both simpler to administer and maintain than their secure counterparts.

- **Flexibility**. It is easy to modify this design to accommodate other needed features. The original classification tables contained no data pertaining to color. When colors needed to be associated with classifications, the tables were quickly modified to provide this information.

- **Portability.** This strategy can be easily ported to other RDBMS such as INGRES and ORACLE. Creating the tables and modifying the queries is accomplished with the same code for all of these RDBMSs. The translation algorithms are written in Embedded C/SQL, which also can be used in all major commercial databases.

- **Vendor Independence**. Unlike other commercial products, secure operating systems are not well supported and maintained by the vendors. The decision to build a simple solution provides a means of avoiding this reliance on unsupportive vendors.

Conclusion (U)

~~(FOUO)~~ Security is the Agency's middle name and must always be applied to its resources. As the workforce gains computer awareness, one of our greatest resources, the vast pool of information residing on Agency computers, is increasingly vulnerable. Many measures can be taken to protect this information; the BOXOAK solution described is one approach that makes sense for its requirements. Every system must make a thorough assessment of its security needs and find the appropriate tools to safeguard its data. Publicizing and sharing our solutions lets us maximize reuse and accomplish security with a minimum of effort.

~~(FOUO)~~ *Ms.* [redacted] *started her Agency career twelve years ago as acomputer systems intern. Since then, she has worked in a varietyof areas, including finance, configuration management support, and collection, usually in database-intensive development efforts. Ms.* [redacted] *currently works in K254 as the software development manager for CADENCE, a new dictionary tasking system for DO analysts and dictionary managers. She also enjoys contributing to the Agency's technical health by teaching at the NCS, mentoring interns, participating in software process improvement activities, and writing this paper.*

P.L. 86-36

Kλ

An Appeal From the Editor:

REORG HAPPENS!

~~(FOUO)~~. . . and once again CRYPTOLOG finds itself with an outdated distribution list.

~~(FOUO)~~ We are frantically trying to update the list from the various announcements that circulate, but since organizations often combine as well as appear and disappear, this is not really a solution. Once CRYPTOLOG's home page is updated to reflect the recent P Staff reorganization, the distribution list will be available for viewing so that organizations can notify the editor of changes in the number of copies needed. Until then, we ask for your patience and cooperation if the wrong number of copies arrives in your organization. Please inform the editor of any necessary changes. Individual subscribers, as always, should inform the editor when their organizational designator changes. (For those who are puzzled by this distinction, the print plant no longer sends out copies to individuals or to organizations below the branch level; this is done by the CRYPTOLOG office.)

Editorial Policy:

(U) Technical articles are preferred over those relating to management, shorter over longer (under 3,500 words). Emphasis should be on improving NSA's technical performance; articles should be aimed at explaining developments in one's career field to thosE outside it. Readers are invited to contribute conference reports and reviews of books, articles, software, and hardware that relate to our missions or to any of our disciplines. Editorials are also welcome, as is humor. Submissions may be published anonymously, but the identity of the author must be known to the editor.

Submitting Articles:

(N.B. If the following instructions are a mystery to you and your local ADP support is no help, please feel free to contact the CRYPTOLOG editor on 963-5283s or cryplog@p.nsa.)

~~(FOUO)~~ Send a soft copy via e-mail to **cryplog@nsa**, or send a hard copy accompanied by a labelled diskette to the editor at P02 in 2C099, Ops. 1.

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, your name, organization, building, and phone number.
- FrameMaker format is preferred; ASCII text is also fine. *(FrameMaker users: please do not put graphics in Anchored Frames as these are nearly impossible to reformat to our standard.)* J334 has a conversion service that converts Interleaf, WordPerfect, OfficeWriter, and MS Word into FrameMaker. Just attach the document to an E-Mail Compose Window addressed to **convert@nsa**.