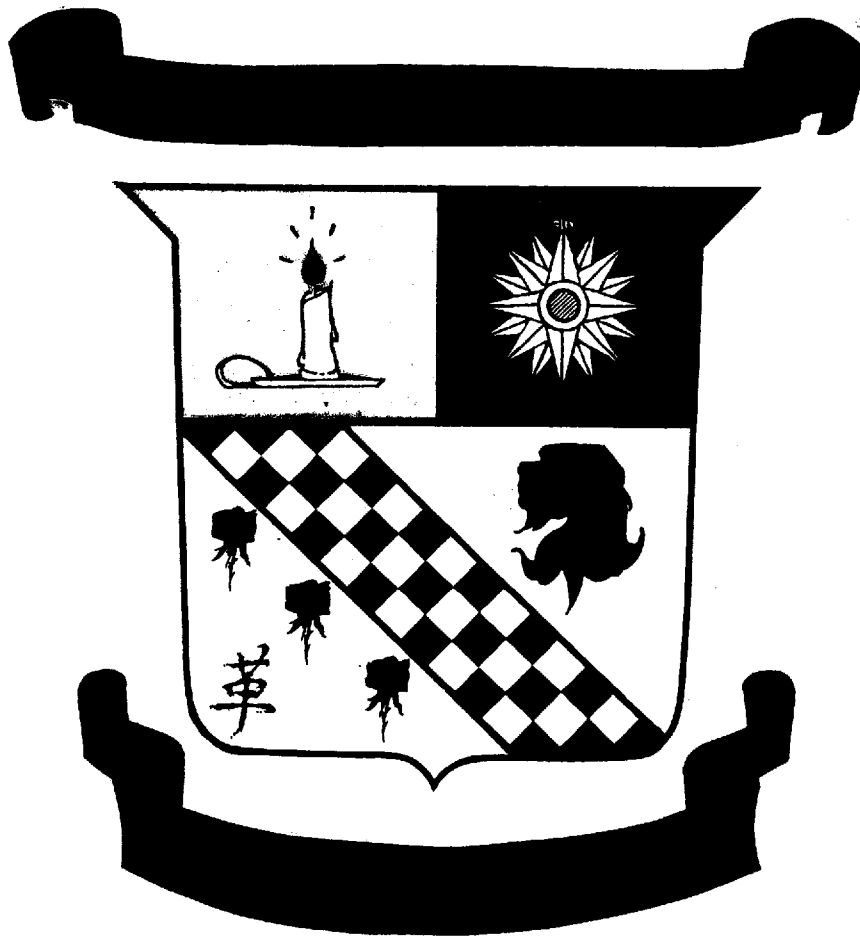


**TESTIMONY AND COMMENTS ON
EXECUTIVE ORDER 12356, "NATIONAL SECURITY
INFORMATION"**

BY

**ROBERT D. STEELE, PRESIDENT
OPEN SOURCE SOLUTIONS, INC.**



**FOR THE
PRESIDENTIAL INTER-AGENCY TASK FORCE ON
NATIONAL SECURITY INFORMATION
DEPARTMENT OF JUSTICE
9 JUNE 1993**

Warning Notice

Security clearance for this material is pending. It should be treated as "For Official Use Only".

It may be shared with any government employees or contractors supporting the Presidential Inter-Agency Task Force on National Security.

It should not be shared with foreigners, journalists, or others external to the Presidential and Inter-Agency Task Force deliberation process.

Table of Contents

- A TESTIMONY on Executive Order 12356, "National Security Information", before the *Committee on Excessive Classification, Presidential Inter-Agency Task Force on National Security Information*, Department of Justice, 9 June 1993, 1145-1200.:
- B COMMENTS on Executive Order 12356, "National Security Information", *Federal Register* Volume 47, Number 66, Tuesday April 6, 1982.
- C *COLLOQUY* (May 1993), a publication of the Security Affairs Support Association (containing transcripts of public remarks by Robert J. Kohler, William Schneider, Kenneth C. Bass, III, Randall Fort, others)
- D Robert D. Steele, "Ethics, Ecology, Evolution, and Intelligence", *Whole Earth Review* (Fall 1992), pp 74-79
- E Robert D. Steele, "Getting It Right, Part I: General Evaluation of National Intelligence Capabilities", *Intelligence and Counterintelligence Journal* (forthcoming issue, Summer 1993)
- F Robert D. Steele, "Getting It Right, Part II: Intelligence Primer--How to Inform Policy", *Intelligence and Counterintelligence Journal* (forthcoming issue, Summer 1993)
- G Robert D. Steele, "Corporate Role in National Competitiveness: Smart People + Good Tools + Information = Profit", *Harvard Business Review* (under consideration).
- H Robert D. Steele, "Recasting National Security in a Changing World", *American Intelligence Review* (Summer/Fall 1990), reprinted in United States Marine Corps, *INTELLIGENCE: Selected Readings--Book One* (Marine Corps University, Quantico, AY 1992-1993) pp. 42-49. Hereafter USMC *INTELLIGENCE I*.

- I Robert D. Steele, "Applying the 'New Paradigm': How to Avoid Strategic Intelligence Failures in the Future", *American Intelligence Journal* (Autumn 1991), reprinted in USMC *INTELLIGENCE I*, pp. 50-53.
- J Robert D. Steele, "The National Security Act of 1992", *American Intelligence Journal* (Winter/Spring 1992) reprinted in USMC *INTELLIGENCE I*, pp. 54-60.
- K Robert D. Steele, "Intelligence Support for Expeditionary Planners", *Marine Corps Gazette* (September 1991), reprinted in USMC *INTELLIGENCE I*, pp. 77-83.
- L Robert D. Steele, "National Intelligence and the American Enterprise: Exploring the Possibilities", Intelligence Policy Seminar Working Group #3, John F. Kennedy School of Government, Harvard University, 14 December 1991
- M Robert D. Steele, "United States Marine Corps Comments on Joint Open Source Task Force Report and Recommendations, Working Group Draft Dated 6 January 1992"
- N Robert D. Steele, "Marine Corps Trip Report: Technology Initiatives Wargame 1991, Naval War College, Newport RI, 21-25 October 1991
- O Robert D. Steele, "C4I Campaign Plan: Proposed Changes in How We Do Business", C4I Department, Headquarters, U.S. Marine Corps, 16 July 1993
- P Biography of and List of Publications by Robert D. Steele

OPEN SOURCE SOLUTIONS, Inc.
International Public Intelligence Clearinghouse
1914 Autumn Chase Court
Falls Church, Virginia 22043-1753

Voice: (703) 536-1775 | Facsimile: (703) 536-1776
INTERNET: steeler@well.sf.ca.us

TESTIMONY of
Mr. Robert D. Steele, President & Owner
OPEN SOURCE SOLUTIONS, Inc.
to
Presidential Inter-Agency Task Force on National Security Information
Department of Justice, 9 June 1993

ELIMINATING EXCESSIVE SECURITY WILL SAVE MILLIONS IF NOT
BILLIONS OF DOLLARS

In my judgement, the Committee on Excessive Classification is the most important of the Task Force committees, because we can eliminate 75% of our security issues, and save millions if not billions of dollars by eliminating excessive classification. Savings will be seen not only within the intelligence community, but also--through improved dissemination of more information--in the rest of the government and in the private sector. There are three kinds of waste caused by excessive classification.

THREE KINDS OF WASTE: SYSTEM COST, POLICY COST,
FUNCTIONAL COST

System Cost: Protection Over-Runs, Handicapping of Personnel

First, there is system cost, the waste of millions of dollars in creating Sensitive Compartmented Information (SCI) information handling systems, with their emission controls, restricted access areas, employee clearance costs, and so on, only to find that 75% of the information processed is in fact unclassified or of a lesser classification.

I will tell you in a moment about my ten million dollar mistake as the senior civilian responsible for standing up the Marine Corps Intelligence Center.

What I want to emphasize at this point is not only the cost of excessive protective measures, but the imposed cost of measures which prohibit our intelligence specialists from obtaining direct access to unclassified systems, from traveling to the Soviet Union, or even something so simple as consulting "uncleared" scholars and foreign experts. We are handicapping our best collectors and analysts--including our collectors and analysts in the private sector. We are preventing them from being effective.

We have created a security bureaucracy which has lost sight of its purpose, and has no idea how to deal with the changed circumstances in the world. Worse, we have an entire community of operations and analysis personnel who have been trained by rote for decades, and do not have a strong foundation for questioning and improving our existing processes. I will give you a vignette here as well.

Policy Cost: Lost Opportunities, Reduced National Competitiveness

Second, there is policy cost, the waste of millions of dollars in lost opportunities for executive action, and the cost of mis-informed policy, which is a direct result of over-classification which makes information too time-consuming for the policy-maker to consider. I will graphically portray how policy-makers make judgements using intelligence based on less than 2% of the available foreign information, and how policy-makers actually rely most heavily on the 90% of the information they receive which is unclassified and unanalyzed. One of the greatest myths of intelligence is that it is actually useful to the policy-makers--in my experience, most policy-makers don't have the time to read their intelligence materials, and very little of what we produce lends itself to strategic application.

Perhaps even more severe, however, is the reduced competitiveness of our Nation, whose citizens--workers, students, others--have an impoverished "information commons" because our national intelligence community contributes nothing to our larger community's knowledge of the world we live in, and the factors affecting international economic and cultural competition and confrontation. In the age of information warfare, it is the people of the

Nation who are the "front-line troops". We have left them blind, dumb, and ignorant. We have no national knowledge strategy. Your efforts to address excessive classification should be the first step in substantially re-inventing our intelligence community so that it is in the service of the Nation as a whole, not some bureaucrat's arbitrary identification of the "top 100" federal executives.

Excessive Classification: The Cement Overcoat of the Bureaucrat

Finally, there is the functional cost, the waste of millions--and more likely billions--of dollars creating massive classified collection systems whose collection we cannot process and whose product we cannot disseminate as widely as necessary to actually influence policy at the working level. There are two major costs in this area. The first results from erroneous or excessive classification. I am certain, and others more senior than I, including members of the National Security Council, have commented on this point, that no less than 75% and perhaps as much as 90% of our classification is motivated by a desire to protect turf, not national security. Erroneous classification also results from tens of thousands of poorly trained employees who routinely classify information by rote, adopting the most conservative route because the bureaucratic penalties for under-classification are severe, while there are no penalties at all for those guilty of excessive classification.

The second cost, most easily corrected, results from embedded classification, where as much as 75% of the information in a document might be unclassified or of a lower classification, but is classified at the highest level of any paragraph in the total document--this effectively removes all of that unclassified information from the broader government library of information accessible to most government and private sector employees. This is the "cement overcoat" of intelligence, burying its perceived competitor, unclassified information, deep within highly classified documents which cannot be widely disseminated.

Intelligence Microscopes, Like Mainframes, Can Become Relics

The reality--and I have published extensively on this topic--is that we have built an enormous classified microscope good only for looking at the strategic nuclear threat in the former Soviet Union, and useless against economic or other targets, even in the former Soviet Union. The failure of the intelligence community to predict the fall of the Berlin Wall, and the

fragmentation of the Soviet empire, is a direct result of our over-reliance on narrow classified systems whose validity and utility were not subject to sufficient scrutiny and oversight.

We have lost sight of the traditional art of scholarship. Our intelligence community, secure with an arrogance born of the privilege of deciding which policy-makers "qualified" for their secrets, has virtually no capability for rapidly collecting, processing, and disseminating unclassified, public information, what we call "open source" or open source intelligence (OSCINT). Excessive classification has created an ossified intelligence community which is now in grid-lock, unable to cope with fleeting and rapidly changing threats and opportunities.

SOME REAL-WORLD EXAMPLES

Now for my quick vignettes:

My Ten Million Dollar Mistake

In 1988 I was selected to be the Special Assistant to the Director, double-hatted for nine months as the Deputy Director as well, of the USMC Intelligence Center. We were given twenty million dollars to spend over a five year period, of which ten million was spent building an SCI-high system required to directly access SCI information from the major intelligence agencies. Imagine our shock when we turned that wonderful system on, and discovered that the national intelligence community does not have any significant data about the Third World, nor about factors of extreme importance to the Marine Corps, such as bridge loading data, port and airhead suitability, and so on. Imagine our chagrin when we learned that most of what we needed was available from commercial information services. Bottom line: we should have spent 80% of our money on unclassified information handling tools and access to commercial data bases, and 20% on couriers and limited access to hard-copy products from the intelligence production centers.

All Those Billions, And We Only Get 2% of the Information

In 1990 I was selected to attend the Harvard Executive Program, and specifically the Intelligence Policy Seminar. There, taught by such talented individuals as Greg Treverton, now Vice-Chairman of the National Intelligence

Council, I refined ideas I had formed earlier through participation in the CIA's "Intelligence Successes and Failures" course, and through my own graduate thesis on strategic and tactical information management for national security".

The problem is one of two parts:

We Collect Less Than 10% of the Available Information

The first part focuses on collection. The fact is that in any given country, we collect less than 10% of the available information. I can provide more detail on this later, but you can imagine how difficult it is, with officers who rarely have mastered the local language, have little time to read, and are consumed with representational responsibilities to truly get an in-depth picture of any given area. Of that 10% that does get collected, it is my judgement, based on experience in three overseas embassies, that 80% gets "spilled" on the way back to Washington. Excessive classification is certainly one of the culprits here, for often information is classified based on who collected it, not whether the information itself is classified. Another is practical. Messages have to be coordinated, hard-copy to parent agencies does not. So many officers, regardless of agency affiliation, opt for the route that is bureaucratically easy, but which actually deprives the broader community of access to the information. So I conclude that all of our collection efforts, both classified and unclassified, actually provide the policy-maker with less than 2% of what is available. I also conclude that increased emphasis on the collection of unclassified information which can be readily shared throughout the government and with the private sector, would allow us to significantly reduce costs--and political risk--associated with clandestine collection, while also significantly increasing the disseminability and therefore the utility of that information.

We Spill or Can't Process 80% of What We Collect

The second part focuses on production. That 2%, by and large, gets turned into intelligence or refined staff products which others, including the director of the CIA's "Intelligence Successes and Failures" course, have concluded constitute less than 10% of the input to the policy-makers understanding of his or her world. Let me stress this: the flood of classified information that we produce not only does not get read by the intended recipient, the policy-maker, but often, because of its excessive classification,

cannot be read by the subordinates of the policy-maker normally charged with digesting and distilling incoming information for the policy-maker.

The other 90% of the input is unclassified, unanalyzed by intelligence professionals, and provided by bureaucrats, lobbyists, Congressional Members and staff, foreign government officials, friends, and family. And of course the media.

There is something very disturbing about this picture. It suggests that the intelligence community has renounced its originally intended mission of informing policy, and been consumed by the passionate (and like passion, often oblivious) desire to focus on secrets for the sake of secrets. I cannot tell you how many times I have heard warfighters complain about intelligence that is too much, too late, too compartmented, and virtually useless.

Lastly, I will mention the over-all failure in developing processing and dissemination capabilities commensurate to our classified collection capabilities. Such authorities as Dick Kerr, former Director of Intelligence for the CIA, and most recently the Executive Director, have been frustrated by the penchant of Congress and the industrial base to push large expensive (and highly classified) collection systems, without providing for the processing and dissemination of those products, or the more mundane collection of unclassified information. A few years ago a senior manager at the National Security Agency told me he processed less than 6% of the signals his group collected. I have heard similar percentages, under 10% for classified imagery.

No Strategy, No Clear Idea of Who Needs What

In my years of service, and especially in the past five years when I have been the Marine Corps member of the Foreign Intelligence Priorities Committee, the Future Intelligence Requirements Working Group, the Council of Defense Intelligence Producers, and other key forums for establishing direction, I have been appalled how we do business. We literally go through the motions. We don't have a strategic plan for intelligence collection designs and methods, and there is little likelihood that intelligence community leadership will produce such a plan in the near future. This is important to you because excessive classification is inherent in the way we do business now, and likely to continue unchecked unless the President receives substantive recommendations to drastically reduce funding for classified systems, and

increase funding for unclassified collection, processing, and dissemination capabilities. If the President will not pay attention to this problem, we will continue to waste millions, perhaps billions, on systems that do not lend themselves to non-conventional targets, and whose cost is multiplied many times over because of excessive classification.

I wish to conclude my brief oral testimony with two comments:

Fiscal Decline Is A Most Refreshing Tonic

First, fiscal decline is a most refreshing tonic, to borrow a turn of phrase from Winston Churchill. It brings out new perspectives, and forces objective reevaluation. When Robert Kohler, a senior TRW officer and former head of the CIA office responsible for building satellites, stands up and says he thinks we can declassify most of what we do in imagery; when William Schneider, former Undersecretary of State, says we should eliminate export controls on our intelligence technologies; when Ken Bass, first Council for Intelligence in the Department of Justice states publicly that most of what he has reviewed is over-classified, then indeed, a breath of fresh air is stirring in the musty vaults. It will not be easy, changing the way we do business. The one bright hope is that Congress will respond to the desire of contractors to sell their intelligence systems overseas, and accede to the declassification of much of what we do so that it can be exported. This in turn will lead to a scrub-down, in which our systems are forced to compete with foreign satellites and other capabilities.

It's Time For Intelligence Managers to Demonstrate Returns on Investment, or Go Out of Business

Second, and here I want to paraphrase a warfighter who spoke to me at Newport in 1991 when we tested our intelligence concepts--he may have been the commander of the lead wing going into Beirut during the war in Southwest Asia-- he said something along the lines of: "If it's 85% accurate, on time, and I can share it, then that is a lot more useful to me than an SCI compendium that is too much, too late, and needs a safe and three security officers to move it around the battlefield". There are unquestionably some things that must always be done by sensitive technical means or can only be obtained through clandestine collection, but on balance I believe that between 75% and 80% of our national policy-makers intelligence needs, as well as the intelligence needs

of the broader consumer base which we have ignored all these years, both the rest of government and in the private sector, can be satisfied with unclassified intelligence which is vastly faster to get and cheaper to process, and has the two additional advantages of being risk-free, and eminently suitable for dissemination to Congress, the press, and the public.

Until the intelligence community is forced to utilize unclassified information as its "source of first resort" (a marvelous phrase coined by Paul Wallner the first Open Source Coordinator appointed by the Director of Central Intelligence); and until the intelligence community is forced to produce unclassified products to the maximum extent possible, then we will continue to waste millions if not billions, deprive most government officials, private sector officers, and citizens of the fruits of our intelligence effort, and blindly pursue secrets for secret's sake, rather than informed policy.

Alvin Toffler and Stevan Dedijer, Harlan Cleveland and Robert Carkhuff, Howard Rheingold and Peter Drucker--each of these authorities has addressed the age of information warfare, of the knowledge executive, of the "gold collar worker", of the privatization of intelligence. The fact is that much of what we need in the way of intelligence is being produced by private organizations as a commercial endeavor--and this includes satellite imagery and signals collection. It is time for intelligence community managers to demonstrate returns on investment, or go out of business. It is time for them to decide if they are in the business of secrets, or the business of informing policy. We need to help them with that decision by redefining what constitutes a "secret", and indeed, what constitutes "national security".

I have attached to the transcript of my testimony a detailed critique of Executive Order 12356 as now written, various articles pertinent to your role in restructuring the way the intelligence community does business, and a personal biography with a list of my recent publications on intelligence restructuring. I have other documents relevant to the proposition that we must re-orient our entire intelligence community toward the mission of informing policy and producing largely unclassified intelligence; these I will supply if requested. May I respond to any questions?

Attachments:

- A Critique of Executive Order 12356, "National Security Information", *Federal Register* Volume 47, Number 66, Tuesday April 6, 1982.
- B *COLLOQUY* (May 1993), a publication of the Security Affairs Support Association (containing transcripts of public remarks by Robert J. Kohler, William Schneider, Kenneth C. Bass, III, Randall Fort, others)
- C Robert D. Steele, "Ethics, Ecology, Evolution, and Intelligence", *Whole Earth Review* (Fall 1992), pp 74-79
- D Robert D. Steele, "Getting It Right, Part I: General Evaluation of National Intelligence Capabilities", *Intelligence and Counterintelligence Journal* (forthcoming issue, Summer 1993)
- E Robert D. Steele, "Getting It Right, Part II: Intelligence Primer--How to Inform Policy", *Intelligence and Counterintelligence Journal* (forthcoming issue, Summer 1993)
- F Robert D. Steele, "Corporate Role in National Competitiveness: Smart People + Good Tools + Information = Profit", *Harvard Business Review* (under consideration).
- G Robert D. Steele, "Recasting National Security in a Changing World", *American Intelligence Review* (Summer/Fall 1990), reprinted in United States Marine Corps, *INTELLIGENCE: Selected Readings--Book One* (Marine Corps University, Quantico, AY 1992-1993) pp. 42-49. Hereafter USMC *INTELLIGENCE I*.
- H Robert D. Steele, "Applying the 'New Paradigm': How to Avoid Strategic Intelligence Failures in the Future", *American Intelligence Journal* (Autumn 1991), reprinted in USMC *INTELLIGENCE I*, pp. 50-53.
- I Robert D. Steele, "The National Security Act of 1992", *American Intelligence Journal* (Winter/Spring 1992) reprinted in USMC *INTELLIGENCE I*, pp. 54-60.

- J Robert D. Steele, "Intelligence Support for Expeditionary Planners", *Marine Corps Gazette* (September 1991), reprinted in USMC *INTELLIGENCE I*, pp. 77-83.
- K Robert D. Steele, "National Intelligence and the American Enterprise: Exploring the Possibilities", Intelligence Policy Seminar Working Group #3, John F. Kennedy School of Government, Harvard University, 14 December 1991
- L Robert D. Steele, "United States Marine Corps Comments on Joint Open Source Task Force Report and Recommendations, Working Group Draft Dated 6 January 1992"
- M Robert D. Steele, "Marine Corps Trip Report: Technology Initiatives Wargame 1991, Naval War College, Newport RI, 21-25 October 1991
- N Biography of and List of Publications by Robert D. Steele

OPEN SOURCE SOLUTIONS, Inc.
International Public Intelligence Clearinghouse
1914 Autumn Chase Court
Falls Church, Virginia 22043-1753

Voice: (703) 536-1775 | Facsimile: (703) 536-1776
INTERNET: steeler@well.sf.ca.us

COMMENTS on
Executive Order 12356, "National Security Information"
by

Mr. Robert D. Steele, President and Owner
OPEN SOURCE SOLUTIONS, Inc.

for
Presidential Inter-Agency Task Force on National Security Information
Department of Justice, 9 June 1993

National Security Information Should NOT Be Classified "By Definition"

The most fundamental flaw of the Executive Order as written is that it equates national security information with "classified information". No where have I ever seen it written that intelligence must be classified, nor have I seen it demonstrated that information of importance to the Nation must of necessity be classified. I have in fact, in resigning from government two years short of retirement, dedicated myself to demonstrating that the opposite case is true: that the wealth and health of the Nation depend much more on a public intelligence capability, a capability to collect, process, and disseminate unclassified information.

Classification Definitions Correct But Insufficient and Ignored

The existing definitions of "Top Secret", "Secret", and "Confidential" are adequate in theory, but are rendered irrelevant because of the complete lack of Presidential direction as to how one should define "national security", "exceptionally grave damage", "serious damage", or "damage". The fact of the matter is that the agencies considered to be part of the national security apparatus have taken it upon themselves to define everything they do,

everything about them, to "be" vital to national security, and they have taken it upon themselves to classify everything about themselves, their operations, and their products, without regard to the definitions established by the President in this Executive Order.

Unclassified Information ("The Competition") Is Buried In A "Cement Overcoat" of Classified Information, Making It Unusable By The Consumer

In my experience, at least 50% of what the intelligence community does is unclassified--unclassified sources, unclassified methods, unclassified products. Unfortunately, because of the total discretion allowed to the community, all that is unclassified is buried, literally, inside of tightly controlled documents bearing the classification of the most sensitive piece of information. Many senior analysts and intelligence community managers have commented on this problem--the President's own intelligence daily frequently contains unclassified information that cannot be released to Congress or the press because it is not identified as unclassified and is contained in a classified document.

A specific example from my experience: as a resource manager at Headquarters Marine Corps, I was party to a contracted effort to review Marine Corps capabilities and limitations with respect to communications, computers, and intelligence in support of each of the theaters. Despite my direction to the contractor that the product be unclassified (I specified "For Official Use Only", we ultimately received a three-inch binder classified "Secret". Upon examination it became evident that the entire volume, with the exception of about twenty pages on "deficiencies" was unclassified. The Executive Order, Section 1.3(a)(2), is being used as the basis for obscuring fundamental information needed to mobilize support for correcting generic deficiencies.

The general categories of information eligible for classification, as set forth in Section 1.3 of the Executive Order, are good ones, but require much stricter definition and oversight.

Employees Have Not Been Trained to Exercise Discriminate Classification

It has been my experience that employees of the various intelligence community organizations routinely classify everything they collect, everything

they write. This is in part because there are severe penalties for under-classifying information, and there are no penalties for over-classification, even if over-classification is against the public interest.

**Firm Limits on the Duration of Classification Urgently Needed:
Two Years (Confidential), Five Years (Secret), Ten Years (Top Secret)**

I believe that specific limits should be set on the duration of classification. This is the "age of information", and the laws of cybernetics rather than the laws of physics are now paramount. The "half-life" of information, even classified information, gets shorter every year. In my judgement, a new Executive Order should, in addition to providing much firmer direction on what constitutes "national security" and "damage", must also specify that with certain strictly limited and supervised exceptions, all classified information is automatically declassified when it reaches ten years of age. Confidential should be declassified after two years, Secret after five, Top Secret at between seven and ten years depending on the topic and country.

**Violation of the Prohibition on the Use of Classification to Conceal
Impropriety or Questionable Activities Appears Routine, Without Sanction**

It appears to me that the prohibition established in the Executive Order, against the use of classification in order to conceal violations of the law, inefficiency, or administrative error, and so on, is itself violated with frequency, whether by design or by habit. The following quotation from a former member of the National Security Council is instructive:

"Everybody who's a real practitioner, and I'm sure you're not all naive in this regard, realizes that there are two uses to which security classification is put: the legitimate desire to protect secrets, and protection of bureaucratic turf. As a practitioner of the real world, its about 90 bureaucratic turf; 10 legitimate protection of secrets as far as I'm concerned."

That observation was made by Rodley B. McDaniel, then Executive Secretary of the National Security Council, to a Harvard University seminar. He was quoted in Thomas P. Croakley (ed), *C3I: Issues of Command and Control* (National Defense University, 1991), on page 68, and again in my

own "C4I Campaign Plan: Proposed Changes in How We Do Business" (C4I Department, Headquarters U.S. Marine Corps, 16 July 1992), page 8.

As an initial remedy against over-classification, I would recommend three measures:

First, integration of training on the revised Executive Order and the intent of the President regarding classification, into the training program of all government employees and their industry counterparts. The training model established in relation to Executive Order 12333 stands as proof that reaching individual employees can make a difference.

Second, elimination of "delegated" authority. In my experience, employees at the very lowest levels of the intelligence community routinely classify documents, and are given the identify number of the person in their chain of command who does have delegated authority to classify documents. They type that is just as if the person had seen the document and approved its classification. Instead, in conjunction with the training program, we need to make the originator of the document, however junior, accountable for its classification.

Third, a much stronger program of oversight, beginning with a complete review of all intelligence production including the daily current intelligence products provided to the President and his senior staff. Measures should be adopted with prevent unclassified information from inheriting the classification of companion information which is legitimately classified, and sanctions should be imposed on organizations which persist in this practice.

Routine Declassification Simply Does Not Happen

Although the existing Executive Order calls in Section 3.1 for the declassification or downgrading of information as soon as national security considerations permit, this provision is, in my experience, ignored in its entirety within the national intelligence community. All documents are classified for the maximum period possible, and all documents which can be exempted from automatic declassification are exempted. This is not done for malicious reasons--it is done for bureaucratic convenience, for it is far easier to "play safe" and have one (maximum) standard, than to train and support employees in applying discretionary judgement.

Intelligence Security Oversight Office Has No Teeth, Has Been Ineffective

I have never, in eighteen years of experience, encountered a representative of the Intelligence Security Oversight Office, or heard of a spot check of any documents associated with any office I have ever been associated with. Although Section 5.2 provides the Office with the authority to conduct on-sight inspections, this does not appear to be a common practice.

In my experience, the Information Security Oversight Office has been a "zero", irrelevant and ineffective. It needs teeth--a staff, and the authority to spot check. It should pay particular care to the over-classification of information which was unclassified to begin with, but which was classified to justify a report by an intelligence agency (instead of turning it over to another government agency), to "protect" the collection agent (whose identity could easily have been obscured or deleted), or which has been buried by attaching relatively minor but more classified material to it.

Across the Board Evaluation Required: Need to Focus on Existing Unclassified Sources, Methods, and Products. Prevent Their Being "Buried" by Classified

I strongly recommend an across the board evaluation of intelligence community collection, external research and analysis, and production, to determine the percentage of sources, contracts, and products which are inherently unclassified, but whose value is being lost because of the excessive classification environment in which the unclassified information is being exploited. In my view, any document which is comprised of 50% or more of unclassified materials, should be split in to an unclassified primary document with a classified appendix.

No Exemptions to Access Regulations Should be Permitted

I find the exemption of the President and his staff from the provisions of Section 3.4(a) to be offensive and contrary to democratic principles. The President and his staff should have the same authority to classify information as the national security agencies, but they should not be exempted from declassification review.

Section 4.3 has no rational foundation. Historical researchers should be satisfied by an Executive Order which radically increased the amount and pace

of declassified documents available for public examination. Former Presidential appointees should be held to the same standard as former government employees. If they retain their security clearances and have a need for access, they should be granted access. If they do not retain their clearances, they should not be granted access.

I have the impression that security has been remarkably lax on the many occasions when political appointees have resigned and left their offices with boxes of classified documents. This is intolerable.

Special Access Programs Abused. Source of Enormous Waste of Dollars

The intelligence community has also seriously abused its prerogative, established in this Executive Order, to create special access programs. It has been my experience that special access program lead to enormous waste because they prevent the sharing of normal capabilities and information.

By way of example, I will note that I have met with a number of contractors, each employed under a different special access program, and each charged with creating the ultimate all source fusion workstation. I believe the waste in redundant research & development for information handling by special access programs to be on the order of \$100 million a year.

Section 4.2, permitting the establishment of Special Access Programs by agency heads, should be revised. Agency heads should be permitted to recommend the establishment of such programs, but a single office responsive to the President, such as the Information Security Oversight Office, should be the sole approved authority, and should establish strict "sunshine" provisions.

It is my understanding that the Special Access Programs result in enormous waste in that contractors are required to keep selected employees, documents, and equipment completely isolated, to the point of building separate vaults for them, and are then also subject to the sometimes arbitrary and sometimes capricious dictates of whoever is administering "security" for a Special Access Program. Any future Executive Order, if it permits Special Access Programs, should establish guidelines which prevent agencies from imposing unreasonable demands on contractors.

Fundamental Premise of the Order Must be Changed:
Information is Most Useful to the Nation When Widely Disseminated,
Should Not be Classified Without Cause

As a final comment, I would state my belief that any Executive Order promulgated in the future should begin with the premise that information, including intelligence, is most useful when widely disseminated, and that information must be considered unclassified until a solid case for its classification can be established. That is not the practice today.

OPEN SOURCE SOLUTIONS, Inc.
International Public Intelligence Clearinghouse
1914 Autumn Chase Court
Falls Church, Virginia 22043-1753

Voice: (703) 536-1775 | Facsimile: (703) 536-1776
INTERNET: steeler@well.sf.ca.us

4 June 1993

MEMORANDUM FOR: *OSS NETWORK PRINCIPALS*

Attached is a copy of *COLLOQUY*, the official publication of the Security Affairs Support Association (SASA). It has been reproduced with the permission of MajGen John Morrison, Jr. USAF (Ret), Executive Vice-President of SASA. I am also providing you with contact information for four of the individuals whose words appear in this collector's item. This one issue captures better than any other work I have seen (other than our own *Proceedings*) the changing directions of the U.S. intelligence community and its industrial base. Feel free to mention that I provided you with a copy of *COLLOQUY*, and their telephone numbers).

Robert Kohler (619) 592-3569. Fax (619) 592-3793.

Executive assistant is Larry Prior, formerly of HPSCI. Kohler is going public with his complaint about intelligence community pulling back contract work to protect mediocre employees from being let go, instead of sharing pain with intelligence industrial base. He also makes a good case for how much of our information, including imagery, is seriously overclassified.

William Schneider (703) 524-5522

Former undersecretary of state, he is a principal proponent of releasing U.S. intelligence technology to foreign markets in order to avoid having them develop their own, and to protect our industrial intelligence base.

Kenneth Bass, III (202) 962-8300. Fax (202) 692-8300.

Ken was the first Counsel for Intelligence at the Department of Justice, and has some very well formed views, founded on solid trial and investigation access to thousands of classified documents, about routine pervasive over-classification.

Randall Fort

(703) 525-2572

A very talented person with well-thought out ideas based on experience.

As each of you finds worthwhile articles and documents pertinent to our mutual interest in Open Source Intelligence (OSCINT), I hope that you will pass along a copy. I will list them in ***OSS NOTICES***, and in selected cases will take on the cost of reproducing them and distributing them to my Corporate Sponsors and other principals.

Best wishes,

A handwritten signature in black ink that reads "ROBERT". The letters are stylized and connected, with a long horizontal stroke extending from the end of the word.

Robert D. Steele
President



COLLOQUY

Suite 112

141 National Business Parkway

Annapolis Junction, Maryland 20701

a publication of **SECURITY AFFAIRS SUPPORT ASSOCIATION**

Volume 14 Number 1

May 1993

- * Intelligence and the Industrial Base2**
By: Robert J. Kohler, *Vice President and General Manager*
TRW Avionics and Surveillance Group
- * Issues and Imperatives for the Intelligence Community.....4**
By: The Honorable Donald C. Latham, *Corporate Director*
C³I Programs, Loral Corporation
- * The Chairman's Perspective6**
By: The Honorable Dan Glickman, *Chairman*
House Permanent Select Committee on Intelligence
- * Modernizing Export Regulations for Intelligence,
Intelligence Related and Communications Security
Products and Services8**
By: William Schneider, Jr., *Chairman*
Schneider-Sohn Associates
- * Intelligence Support for Economic Competitiveness10**
By: Kenneth C. Bass, III Esq.
Partner, Venable, Baetjer, Howard & Civiletti
- * Economic Espionage for the Private Sector: You can't
get there from here12**
By: Randall Fort, *former Deputy Assistant Secretary of State, INR*
- * Economic Implications of Information System Security Failures..... 14**
By: Daniel J. Ryan, *Director, Information Systems Security, OSD*

Intelligence and the Industrial Base

Robert J. Kohler

Prologue

In one sense, the following paper is a small part of a much larger issue. What should be done with the NRO, its programs and, hence, its industrial base? This question should ideally be answered in the context of what role intelligence should play in the new world. In a very real sense, the NRO is suffering from the inability of the intelligence community to answer this question. Prior to the collapse of the Soviet Union, the role of intelligence in the security of the nation was clear. Today, it is not clear. Redefining the role of intelligence and its value to the President and the government is a difficult task that has yet to be accomplished. It is a task, however, that must be done. But, there is one large piece of the community (called the NRO) which is in fair disarray. Therefore, starting a dialogue around at least a piece of the problem seems appropriate. It is in this context that this paper is offered.

Introduction

In the debate taking place on the appropriate size of the intelligence budget, one important aspect has been consistently overlooked: the impact of reduced budgets on the industrial base that supports intelligence. Considerable discussion has occurred on the legitimate size and organization of a restructured intelligence community. The contractor world that supports it, however, has been mostly ignored. Industry should not be immune from cuts or the downsizing that must occur. But industry must be downsized in a smart way. This will only be done if it's understood that the industrial base that supports intelligence is as important as the government base and needs to be viewed in that context.

A powerful example is the industrial base that supports the National Reconnaissance Office (NRO). Without industry, there is no NRO. Yet, NRO decisions are made with little thought to the people, capabilities and technologies that support this element of the intelligence community. Today, many thousands of industry employees, who have supported the NRO for years, have been laid off and their critical skills lost. These people and skills have been lost forever as people are choosing to leave the industry rather than face continuing uncertainty in their careers. The problem starts with a lack of a clear understanding as to what (or even why) Satellite Reconnaissance is needed now that the cold war is over.



How Important is Satellite Reconnaissance to This Nation?

The answer to this question is fundamental and is the premise for all resultant discussions. In the past, the premise has been that Satellite Reconnaissance was of the highest priority to this nation's security. Because of that priority, Industry provided its best and brightest personnel to these programs. And because of that same priority, a National Reconnaissance Office was created to provide a focused management of this critical program.

No one questions that NRO programs are important to the nation; however, it is unclear how important they are and how they rank against other intelligence programs and activities. Also, because the NRO programs are visible activities that involve significant chunks of money, they are seen as an easy source to cover cuts in the overall intelligence budget. But, because it is easier doesn't mean it is the right thing to do.

Satellite Reconnaissance is Still Required

NRO programs are still important to the security of the Nation. Daily, we wake up to some new story of conflict in the world around us. There no longer is a brake on ethnic, tribal or religious rivalries. Many of these rivalries could "grow" into national conflicts, but at a minimum, they will challenge the diplomatic, military and leadership position of the United States in the world.

America will continue to have global interests. It is inevitable that United States interests will be engaged and challenged again and again. With the pace of change in the world, our nation will constantly debate what is and what is not a "vital interest" of the nation. What is often missing in the current debate about the future of intelligence, is that this uncertainty will cause further pressure on intelligence (including NRO systems), not make the problem easier.

Increasingly, limited use of U.S. Forces is becoming an option for a variety of missions the U.S. sees as important. Committing U.S. Forces requires a good understanding of the threats or forces they will (or may) face. Satellite reconnaissance remains the best, easiest and most complete way to provide this information. In addition, satellite reconnaissance is the source that can provide a worldwide information base in a systematic, comprehensive and timely way.

Satellite Reconnaissance provides the best capability for timely and worldwide intelligence support. Worldwide coverage will be even more necessary than

(continued on page 3)

(continued from page 2)

before. Our friends and our enemies will be less constant; the location of crises will be less predictable; and the number and types of crises will be more frequent and varied. Other collection assets will never have the responsive and flexible worldwide coverage of satellites, which can shift focus from Baghdad to Serajevo on demand.

With many collection assets (such as Human Intelligence), you must commit to a future operation; the Director of Central Intelligence sends so many agents into so many countries to focus on so many relatively narrow intelligence issues. The Intelligence Community will never have sufficient resources to cover all the needs with agents or conventional collection techniques. With these very few valuable agents we focus on a few valuable targets; and on occasion an agent's life is at risk. There is also the possibility of political embarrassment.

With satellites, we cover the world and prepare for the unknown and the unpredictable. Satellites can cover the world today and then focus on the crisis of tomorrow. The National Reconnaissance Program (NRP) of the past specialized in its ability to penetrate the "denied" regions of the Soviet Union. The NRP of the future will specialize in its ability to rapidly focus on the future crisis and penetrate a temporarily denied area that comes with crisis, conflict, or war. Short of crisis, there will be situations where territory is politically denied to us but we still have a requirement to collect information. Again, the NRP will provide the foundation for our collection efforts.

More often than not, the crisis of the future will find the intelligence community playing "catch up". Because we will have waited too long and do not have a clear idea of what our objectives will be during the early phases of the crisis, there will be a high premium on satellite collected information and its ability to collect information in a "panic". Much of this "panic" collection will be against those radars, communication systems and electronic devices that are coming to dominate the military battlefield. If our nation is to effectively support our military operations and provide the maximum possible guarantee of preserving the lives of U.S. military men and women, then we must dominate the high ground of information. We can best do this with satellite reconnaissance.

Because we will be hesitant to commit any deeper into a crisis than we have to, there will be a premium on intelligence collection with "standoff" capability—able to collect needed information but not risking the lives of intelligence agents or U.S. service men and women. Satellites are politically less risky; no U.S. personnel will be seen held hostage on the nightly news.

Satellites will not intrude on a nation's sovereignty and they bring with them no risk of escalation that is often associated with other collection means. Satellite reconnaissance in this role will still provide critical information to our nation's decision makers as they strive to preserve the peace.

Rhetoric versus Reality

There is currently a gap between rhetoric and reality in the ongoing debate of how to restructure the defense establishment and the intelligence community, while simultaneously reaping the "peace dividend."

First, the rhetoric. The drive to cut the defense budget philosophically assumes greater reliance on intelligence to guard against uncertainty and to give greater warning time for any future crisis. Without this investment in intelligence the current proposals to reduce defense overall, and each of the specific service force structures, could be considered reckless.

But, consider the reality. Funding for intelligence is being reduced, more by Congress than the administration, but they are both beginning to reduce at a pace that will only gain momentum now that the walls between budget categories come down in the current 1994 fiscal year. Many would agree that some programs of the past deserve to be cut. The concern, however, is the future. The world is a very complicated and constantly changing environment. President Clinton and the leadership of our nation deserve to have intelligence collection that will allow them to deal with future challenges and crises.

Not only are overall reductions to the intelligence community too deep, these reductions are falling disproportionately on the investment accounts of research, development and procurement. In the Intelligence Community, reductions are then falling disproportionately on the National Reconnaissance Office. You have to ask, "Why?"

In the National Foreign Intelligence Program (NFIP) there is a survival imperative to protect the civilian manpower growth of the last two decades, even while Defense cuts its force structure and industry proceeds with massive layoffs. Any new initiative is held hostage to maintaining base programs which form a cocoon around the manpower growth of the past.

The vast manpower growth in the Intelligence Community needs serious review. It is easier to cut the NRP and let industry hand out the pink slips than to even consider a "reduction in force" across the NFIP. Programs are canceled; thousands are laid off in industry; yet the numbers in government remain relatively the same.

There is much movement within government to "reorganize". In industry we do so to gain efficiency, reduce overhead and reduce the number of people we employ. This is even more important in the "down market" that we will be living with for the foreseeable future. The Intelligence Community needs to study ongoing industry reorganizations; compare with the reductions in the Intelligence Community and the armed forces; and look at how unbalanced these reductions in the Intelligence Community are.

Certainly there are reductions to the NRP that make

(continued on page 16)

Colloquy, May 1993

Issues and Imperatives For The Intelligence Community

by The Honorable Donald C. Latham

In the December 1992 issue of "Colloquy", Richard J. Kerr, the President of the Security Affairs Support Association (SASA), wrote a thoughtful article on the Intelligence Community (IC) and the industry which supports it. His provocative commentary ranged from IC requirements to budgets, the industrial base, investment priorities, and technological innovation. These are compelling issues to both government and industry which deserve the best thinking in some form of joint partnership arrangement. What follows are some additional observations on four of these issue areas and the imperatives they generate.

ISSUE I:

THE INTELLIGENCE REQUIREMENTS PROCESS IN THE IC AND DoD

With a reduced force structure and a complex variety of foreign threats, the Department of Defense (DoD) will continue to be the predominate consumer of intelligence in the federal government. Thus the requirements process should initially focus on Support to Military Operations (SMO) and the development of a slimmed-down, yet capable and responsive core intelligence systems architecture for SMO. To accomplish this, the IC must better understand what the Services, and especially the CINCS, are thinking and where new technology infusion is very rapidly changing tactical warfare. The process is primarily a government responsibility and not something industry can help with except indirectly. More on that later.

Within the IC, the requirements process is still fragmented between the National Foreign Intelligence (NFIP) and the Tactical Intelligence and Related Activities (TIARA) accounts. There is also severe fragmentation within the NFIP and TIARA accounts themselves because of the stovepipe nature of the NFIP agencies that compete for funds, and because the Services compete with each other for TIARA funds.

Every year when the ASD(C³I) testifies to Congress, the issue of NFIP and TIARA coordination is repeatedly raised. Each year the answer is more hand waving than substance on coordination, oversight, and integration of NFIP and TIARA requirements, technology, and ultimately, programs. This still seems to be the case simply because the two accounts are driven by two different masters attempting to preside over a stovepipe set of bureaucracies within their own empires.

The IC requirements process and resulting budget allocations are also strongly influenced by "technology pull" versus stated user requirements. This has not nec-

essarily been all bad, because it has resulted in superb, first-in-its class, national technical systems for imagery and signals intelligence production. As is the case with large DoD weapon system programs, however, once a major intelligence capability is start-



ed it becomes extremely difficult to terminate or significantly redirect. The same is true of the intelligence agencies which produce and operate the systems. Also, the industry which produces these systems constitutes an aggressive and powerful lobby that resists change. This powerful lobby is now trying to argue that preserving the technical industrial base justifies the continuation of existing programs as well as the start of new programs to meet "new" intelligence requirements.

Because the technology pull for 40 years was primarily directed against the Soviet Union, the NFIP processes, systems, and personnel are very target-oriented to the "Soviet problem." Some of these Soviet problem-driven capabilities can be used (and are) to satisfy other requirements, including the non-DoD needs of policy makers and other agencies.

However, from a strategic warning or military threat perspective, it is difficult to justify continuing the technology pull argument to meet shifting and potentially quite different DoD SMO requirements, especially for NFIP-funded systems. U.S. tactical warfare doctrine and tactics are undergoing radical, if not revolutionary, revision driven by two imperatives: (1) the infusion of new technology in platforms, weapons, and C³I; and (2) the change in DoD missions driven by new political priorities and threats to world order.

These imperatives signal to the Intelligence Community that a major shift in capabilities and orientation is required to meet emerging SMO requirements*. The same trend is also true for other intelligence consumers such as Commerce, Treasury, and Agriculture where rapidly shifting commodity markets and other economic/trade decisions by the international community must be known early and acted upon. Thus the IC must gear up to become more responsive to a diverse set of customers who expect better quality, more relevant,

(continued on page 5)

(continued from page 4)

and timelier products.

To do so, the requirements process must be streamlined to permit near real-time input and prioritization of requirements and far more timely response, even to non-DoD users. This will require education of the user community and a major shift in process and attitude of the IC. The IC needs to learn from the commercial world that the customer is king and that satisfaction of customer requirements with a quality product is the only measure of success. That lesson has yet to be learned at either the national or tactical level of intelligence in many people's judgement. For example, despite the fact that DoD has had detailed requirements for years requesting specific systems support to tactical warfare operations, we witnessed significant intelligence ad hoc during Desert Storm which did not satisfy the ultimate user, the CINC and his staff.

Perhaps DCI Woolsey and Secretary Aspin could marshal an objective task force to examine how the commercial market place keeps tab on user trends and requirements in high technology products and services. Who knows? Maybe there are better ways to both generate and satisfy intelligence requirements which could be implemented in the user and Intelligence Communities, with acceptable gain to both!

ISSUE II:

COMPETING BUREAUCRACIES AND WASTED RESOURCES

Competition for ideas and judgments in the intelligence process should be solicited and welcomed. However, the competition among stovepipe intelligence agencies and the services for resources has become so divisive that we are both squandering taxpayer's money and failing to meet valid user requirements for intelligence support.

One factual story of the difficulty a Director of Central Intelligence (DCI) had in dealing with the competing agencies and interest groups in the NFIP occurred during the Reagan administration and involved the National Foreign Intelligence Board (NFIB). The NFIB chaired by the DCI, was a senior intelligence advisory group that met frequently on policy and budgetary issues. Members included the directors, or equally senior officials, of all agencies receiving funding in the NFIP plus the ASD(C³I) representing the Secretary of Defense. By the mid-1980s, it was clear that the very significant annual growth in the NFIP since 1981 was not going to continue. Then DCI Bill Casey was so frustrated with the crowded NFIB meetings (where nothing was ever really accomplished) that he put together a sequence of mini-NFIB meetings to expressly address budget priorities and program allocations. By inviting only five or six agency directors, allowing no staff to be present, and requesting that everyone present take a global view of the issues,

Director Casey assumed that the real priorities and cross-agency budget trade-offs could be rationally addressed.

He was wrong! Despite several mini-NFIB sessions, the process did not work. Those agencies, such as NSA and the NRO, that resided in DoD always invoked their unique SMO requirements and reporting relationships to the SECDEF and Chairman JCS to fend off any prioritization and reallocation of their NFIP budgets by the DCI. If the DCI had unilaterally directed any significant changes in the NFIP outyear budgets, or attempted to terminate or redirect a program he judged of lower priority to something else (even to meet stated DoD requirements), the threat of a direct confrontation with the SECDEF and JCS loomed overhead.

As a result, the DCI was perpetually stymied by bureaucratic budget gridlock and not master of his own responsibilities. The proposed Intelligence Reorganization Act of 1993 would have gone a long way toward addressing this gridlock if enacted into law.

Looking back, it is interesting that even Director Casey with the access and personal relationship he had with President Reagan was unable (or unwilling) to wrest control of the NFIP from DoD except as it pertained to CIA.

Within the TIARA account, the Services and agencies tend to go their own ways with little cross-fertilization of requirements, technology or programs. One of many examples illustrates the problem-the Air Force has spent an estimated three quarters of a billion dollars (\$750,000,000) in developing and fielding the ground based collector management, processing, analysis, and dissemination systems for the TR-1 collection platform. The system is now called the Contingency Airborne Reconnaissance Systems (CARS) which is the new name for the TR-1 Ground Station or TRIGS.

CARS is an all-source (EO/IR/Radar imagery and SIGINT) capable system which can merge and display, for example, an image of a SAM site correlated in time and precise (GPS accuracy) location with an ELINT intercept from that SAM. The CARS is being reconfigured into Air Force tactical shelters which can be configured in modules to meet specific requirements as to type of intelligence and other tactical user requirements.

On the other hand, there is the Army All Source Analysis Stems (ASAS) program which has also spent hundreds of millions of dollars over the last decade to develop an all-source tactical intelligence processing, analysis, and report system - in effect an Army version of CARS - to handle GUARDRAIL and ground based collectors. Some prototype ASAS-I systems have been produced and are in evaluation and test. At the same time, the Army has issued an RFP for ASAS-II with the industry proposals currently in source selection. ASAS-II would be the "objective" systems to support "Army unique" tactical intelligence requirements.

The Army has repeatedly been informed about CARS

(continued on page 18)

The Chairman's Perspective

The Honorable Dan Glickman

"I think these are very, very fundamentally difficult and interesting times. I know far less about my subject matter than those of you in this room do. So, I do not mean to be presumptuous in my remarks, whether you work in the community or whether you toiled outside the community or both. But, I do think we are in a world of great fundamental change. What we do in intelligence, I think, can have a lot to do with easing the transition into a modern world and protecting U.S. interests.

There is the story about a man who works in a big New York City office building. Not the World Trade Center thank God, but another one. Every day he comes out and there is a pretzel stand in front of this office building and a sign on it says 'Pretzels for Sale.' The man would leave a quarter on the stand for a pretzel, but wouldn't take the pretzel. He would do this every single day for weeks and weeks. He'd leave a quarter and not take a pretzel. Finally, one day he is walking by and the old lady that ran the pretzel stand said, 'Well mister I've got to talk to you about something.' The man says, 'I know what you're going to tell me. You're going to tell me that every day I come down here and leave a quarter and don't take a pretzel.' She said, 'No I'm not. I was going to tell you the price went up to thirty-five cents.'

In the process of the last few years the price has gone up. Both in terms of budget exposure, and in terms of world conditions, there have been changes taking place. Our job is to try to do the best under the circumstances, to meet and cope with that. I think, at the same time recognizing that we cannot withdraw from the world, that this world requires the United States of America, which remains the only great moral influence in the world, to keep its international interests and to keep its hand in the world with respect to our goals, which is to promote freedom and democracy and human rights. Not that we are in a position to control events everywhere in the world. We no longer have that power or authority. And besides, economically, we are not the dominant force, singularly, in the world anymore. But, clearly we leave this era, this kind of post Cold War era, or whatever you want to call it, a nation which remains unequalled in the world. It would be a tragic mistake for us to relinquish our power, our leadership, our involvement in the world. And so I think, if we look at the future and look at intelligence operations, I think it has to provide our policy makers with the kind of input and information needed for the United States to maintain its role as the dominant world leader, particularly as the dominant political world leader. We have gone as

a committee all over the world in recent years. I was in Czechoslovakia in 1990 with the Congressional delegation where we met with the Minister of Interior to discuss intelligence issues and how the world had changed. We were talking with the Czech Intelligence Minister, who a few years back had been one of the leading participants in the Soviet system. In Poland in 1990 we met with the Minister of the Interior who briefed the Congressional delegation on the new intelligence structure of Poland. In Yugoslavia in 1990 we were in Belgrade when the embassy there predicted war and massive civil strife in Yugoslavia. But who would have thought the situation would have evolved to where it is today in that part of the world. More recently I visited Greece, Turkey and Israel. All three highlighted their concerns about the changes in the world as a result of the lack of the focus provided by a Cold War primarily engaged in by two clearly acknowledged super powers. I think the point that was made by President Ozall of Turkey, and expressed by all the leaders, men of the three countries, there is no focus in the world now, unless you the Americans maintain yourselves as that focal point. Israel, in particular, has changed views about the new regional threats in these areas.

The intelligence community is faced in this context with many challenges. The first one of course will be in the area of dollars spent in terms of budgets. There is no question we are talking about reduced budgets. How much ought to be determined not just strictly by dollars that are spent but by policy. But, unfortunately in government today, we tend to look at things based on how much money is in the pie, then we divide it up. It is too bad we can't do it the other way. But given the fact that we have very serious budget problems, given the fact we are talking about a deficit this year of \$300 billion, and given the fact that the perception, at least, that the world has changed significantly and doesn't require the same level of intelligence, there is no question that defense and intelligence are going to be viewed very skeptically by folks who want to look at this part of the budget as a large contributor to the deficit situation.

The second challenge is going to be questions and skepticism by Congress and the public about the functions that need to be continued to be performed. Today as you know, we had a hearing. Jim Woolsey did a splendid job. I asked for this hearing. We needed it for my colleagues on the floor who would come up to me and question, 'Why do we need intelligence any more. Why do we need CIA any more. What's the purpose of

(continued on page 7)



(continued from page 6)

all this stuff now. Most of it isn't worthwhile any way.' Some of these people do not have the foggiest idea of what the Intelligence Community does, I'm telling you. You know what it does, but most of the public don't have any idea what it does, and most members of Congress don't really have a very good idea of what it does.

A couple of weeks ago, we took a retreat and went down to the farm. We have a group of new members on the Intelligence Committee in the House, 11 out of 19. We met and General Clapper was there, Admiral Studeman was there and Jim Woolsey was there and we had a former DCI, Bill Colby there. We just sat around and we talked about everything. It wasn't confrontational. It was as much informational, as anything else. What is surprising was how many members came back and said, 'I didn't know they did that. I didn't know they kept this or that nation from getting a nuclear weapon' or 'I didn't know they kept this part of the world stable' or 'I didn't know any of these things.' The fact of the matter is the secrecy involved in intelligence, legitimately kept that way, has in fact boomeranged and nobody knows what it does. Nobody knows anything good that it does. I think that is something that has to change and that was the purpose of the hearing today. It was to get the new director to talk about its achievements, but do it obviously in a way that doesn't jeopardize sources and methods and doesn't do anything foolish.

I thought it was a good first step in what I call demystifying intelligence. Because if it is not demystified it will not last. The pressure is there to slash and cut. Without a common enemy, a central enemy, a focused enemy, more and more members of Congress are going to say, 'What good does it do us. Why can't we get the stuff from open sources. Why can't the State Department do this kind of thing.' So I think it was important to have this kind of hearing and we're going to try to do our best to legitimize to most members of Congress, the important things that the Intelligence Community really does.

Other challenges are: defining the difference between intelligence and information and ensuring that the community assets are focused on the former, intelligence - not the latter. Because we've had a change in operation and change in the world, we just don't want to look for tasks to give the Intelligence Community, that could accurately and responsibly be done by open sources of government. That's not the kind of thing we should be doing. We need to be investing in the right technologies, balancing available resources between investment, maintaining infrastructure, and personnel.

In terms of the Intelligence Committee, again I'm new as Chairman, while I served five years on the committee, I'm learning a lot in the last few weeks that I never dreamed of before in terms of what is done. As I said, this year 11 of our 19 members are new. There is a new chairman and ranking Republican, Larry Combest of Texas. Our committee requires crossovers into Armed Services, Appropriations, Judiciary and Foreign Affairs. We have key members such as Bob Torricelli from New

Jersey and Julian Dixon from California, who crossover into these other areas, including also Norm Dicks of Washington State, who is the second ranking Democrat on the Defense Appropriations Sub-Committee.

I want to work with leaders of the intelligence community to build a consensus that timely and reliable intelligence is essential to our nation's security. Much of the intelligence business is by nature secret. I believe however, that there are ways in which to make known publicly, if only in a general way, some intelligence community activities by which the public can get an idea of the importance of the community's work. In this context the Committee will evaluate the effectiveness of ongoing intelligence operations and activities. It will conduct oversight through all three subcommittees to include legislation, oversight and evaluation, and budget. I see a much greater role for the oversight and evaluation subcommittee this year in reviewing and assessing the performance of the intelligence community. We will ask about duplication — how much is enough and what can we not afford to do any longer? Also, how much can/should the intelligence community do in the economic and environmental areas? In other areas not traditionally the focus of the intelligence community, how much analysis is duplicated, whether it's the Defense Intelligence Agency or the Central Intelligence Agency or other agencies within the community. What, sensibly can we do without and what sensibly do we need duplicated. We'll also be looking at legislative items which could include: legislation dealing with personnel issues, the Classified Information Procedures Act, and intelligence support to law enforcement activities.

The Program and Budget Authorization subcommittee will continue to recommend an annual authorization of intelligence programs. We will be waiting, frankly, to see Mr. Woolsey's recommendations on the budget which he will deliver to us probably later this month. Intelligence budgets have fared very well compared to DoD growth and decline patterns. Last year was the first time Congress cut intelligence deeper (percentage wise) than defense. Such reductions represent a judgment by some members that a budget which had doubled in dollars and in personnel through the 80's, was too large, and the community is over staffed according to some members of the committee. The Committee today, in an open hearing discussed the budget in broad terms with the Director and in a closed session tomorrow we will go into more detail about his priorities and approaches to managing (and reducing) the budget. I don't think we have any preconceived views on the size of the intelligence budget, and I do not expect the Director to have any radical views. If anything today the impression was, at least for the time being, there would not be any radical changes. I frankly think the committee probably will be reasonably cooperative. Not docile, but reasonably cooperative provided he gives us a good long term plan as to where he wants to take the community over the next four or five years. We do have to remember that last year's reductions by the Congress

(continued on page 22)

Modernizing Export Regulations For Intelligence, Intelligence-Related, And Communications Security Products and Services

By William Schneider, Jr.

The fragility of the highly specialized industrial base supporting the U.S. intelligence community is facing the near-term prospect of a significant reduction in its capability to respond to national needs. This is due to the contraction in the domestic market as the overall level of national investment in defense as a fraction of national income declines to pre-World II levels. Unlike other vendors in the defense market, the intelligence/security sector currently lacks options that can sustain the industrial base as the intelligence community is restructured around a diminished resources. Vendors in the intelligence/security sector cannot readily diversify into other sectors of the defense market as these already face dwindling opportunities as the U.S. force structure and associated budgets are reduced. Nor can vendors address opportunities in the international market due to severe export constraints. If this problem is not swiftly addressed, the industry will be obliged to liquidate its excess capacity in facilities as well as personnel — measures which will inevitably diminish the ability of the industry to meet national needs that are not less demanding than those during the Cold War.

The option of using appropriate funds to mitigate the loss of critical capabilities is severely limited. The breadth of capabilities which must be sustained is simply too large to be affordable in the anticipated retrograde budget environment. The selected liberalization of the existing structure of export control regulations affecting the intelligence, intelligence-related, and communications security (COMSEC) markets is the most cost-effective approach to addressing the problem of the intelligence community's industrial base.

Export Policy

Unlike other munitions list items, intelligence, intelligence-related, and COMSEC products and services, exporters find that authorization is normally denied if the export poses a risk to U.S. interests. Other munitions list items are authorized for export when the prospective risk to U.S. interests can be managed in an acceptable manner. Advances in the technology in the intelligence/security sector makes such a conservative approach neither desirable nor necessary. Software drives the performance characteristics of modern intelligence collection and processing systems as well as communications security. When combined with well established license proviso-practices, software manipulation can permit the export of selected systems in a manner that will simultaneously limit the risk posed to U.S. interests while providing market opportunities to sustain the American industrial base for the intelligence

community. Moreover the ability of U.S. industry to dominate the international market will provide the U.S. with a profound ability to shape and influence the proliferation of intelligence security capabilities throughout the world.

Proliferation of Foreign Intelligence and Intelligence-related Systems

The emergence of long-suppressed national and sub-national rivalries as a powerful force in international politics is creating a demand for national intelligence capabilities. The characteristics sought by many international customers pose a potential threat to the ability of U.S. military forces to operate in some environments, and may jeopardize regional stability. Unlike most defense products, foreign producers lack a well developed industrial base to rapidly exploit the range of existing market opportunities. In the long term, the abstention of the United States from this market will produce the opportunities for foreign producers to create an industrial base to address the market demand.

Several foreign producers seek to integrate their existing national capabilities in sensors and platforms with national space launch aspirations to address the most sophisticated end of the market. A larger number of producers appear prepared to address less demanding portions of the market. While the initial offerings are not likely to approach American standards, they will provide the embryonic industrial base, and access to other intelligence organizations that could have a negative effect on American interests. Foreign organizations facing the dilemma of liquidating excess capacity in their development and manufacturing subsidiaries over the next three to five years could find the international intelligence/security market particularly attractive if U.S. export policy is highly restrictive. The consequence of a continuation of current policy is likely to include the proliferation of foreign intelligence and intelligence-related systems.

Techniques to Manage Risk

The performance of collection systems can be shaped by the software which drives system characteristics. The manipulation of performance characteristics can cover a wide range from the general to the highly specific. For example:

- o imagery resolution
- o geographic coverage
- o emissions detected/processed
- o frequency range of emissions

(continued on page 9)

(continued from page 8)

- o modulations characteristics of emissions detected/ processed
- o communications security algorithms processed
- o communications security waveforms
- o maintenance characteristics

End user modification of software-managed performance limitations can be addressed through license provisos. Precedent is already established (e.g. Saudi AWACS) for the parallel ability of U.S. personnel to monitor raw collected data in real time to detect end-user abuse. Foreign purchasers may acquire U.S. intelligence collection/processing systems without providing access to sensor/processor technology. The end user of the system(s) can be constrained through U.S. software manipulation that would allow the system to collect/process information consistent with American interests, while denying the ability to collect/process information contrary to those interests. End users are already "adjusted" to American practice which severely limits the use of defense products to address American policy sensitivities. Korean and Saudi end users have acquired products with limitations on use, deployment, and support. Yet, the end users appreciate that the performance characteristics of systems transferred to them do meet their security needs against a threatening regional actor even if they are denied performance characteristics that would serve their regional aspirations. Manipulation of maintenance requirements can compel the sustaining of a permanent "umbilical" to the U.S. collection and processing capabilities to friendly nations that effectively restrict the performance and end use of the systems to purposes consistent with American interests. In other cases, extensive end use restrictions have been employed including the operation of systems transferred.

Implications for American Interests in Export Policy Liberalization

The world-wide post-Cold War trend to managing national defense is to reduce force structure and personnel end-strength to significantly lower levels is producing a demand for products and services American industry is well-prepared to provide. The generic practice of substituting "capital for labor" is particularly evident in the C³I arena. Nations are prepared to accept the risk associated with lower force levels when they can support their smaller forces with improved C³I to multiply their effectiveness. The United States has the most advanced and comprehensive C³I product range. Its products would be likely to dominate the international market if they could be offered. The absence of U.S. industry from the market in the face of a growing international demand for C³I products and services will stimulate non-U.S. vendors to offer intelligence/security related equipment. Primitive space-based imagery technology already exists in Europe, and a well-financed end-user could readily induce an upgrade in this tech-

nology. Collection/processing technology for airborne manned and unmanned platforms is better developed in Europe and is the type most likely to be offered in the early stages of market development by non-U.S. vendors. Experience in other competitive defense markets indicate that European, Israeli, and Asian vendors seek to exploit market gaps produced by U.S. export regulation. A policy reluctance on the part of the U.S. government to authorize the transfer of software source codes is causing U.S. vendors to lose international markets for key subsystems, and in the future could affect major platforms as well.

Abstention from the intelligence/security market by U.S. vendors would be likely to produce a market for non-U.S. vendors in intelligence/collection processing equipment of modest performance in the hands of many regional actors where such capabilities would be troublesome to American policy. For example, possession of a moderately effective imagery/SIGINT capability of a Gulf nation that we employed in peacetime against Israel would undermine American regional security objectives and diplomatic leverage. Moreover, the creation of a robust international market in products/services denied to U.S. vendors will facilitate the creation of an intelligence/security industrial base outside of the United States that does not serve American interests.

If, on the other hand, American export policy is liberalized, important benefits would accrue to the U.S. intelligence community which we believe would justify the "risk."

(1) The U.S. vendor base for intelligence/security related equipment and services would have an opportunity to sustain its sales volume, work force, capital investment, and profitability to offset or mitigate the decline of these factors in the domestic market. Its ability to serve national needs could continue without degradation arising from contraction of the domestic market.

(2) The U.S. collection/processing effort can be augmented by license provisos which provide U.S. access to collection by allied services. As the number of U.S. bases abroad shrinks, as some technology forces collection closer to the source, and as multilateral, coalition, or international force employment grows, intelligence exchange arrangements will expand greatly. Foreign sales now provide a cheap way to initiate these exchanges and to explore technological approaches to limiting and controlling them.

(3) The U.S. can retain an important measure of control/influence over the evolution of foreign systems if American systems are used.

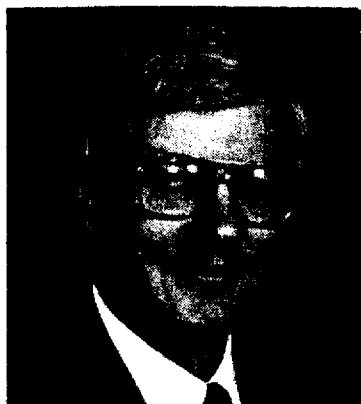
(4) An aggressive American international marketing posture can severely limit the ability of European/Israeli/Asian vendors to develop an industrial base in the intelligence/security field assuring the U.S. of a "quasi-monopoly" on high performance devices in this sensitive arena.

(5) By developing a "high volume" production base

(continued on page 21)

Intelligence Support For Economic Competitiveness

by Kenneth C. Bass, III, Esq.



The title of this section of the SASA Spring Symposium reflects a profound change in the international situation over the past 15 years. Each of us grew up in a world in which the United States became the strongest military power and was constantly confronted by another military power with the capacity to physically destroy our society. In that world we created an intelligence community and defined its role as the support of military supremacy and informed foreign policy. Throughout the past 50 years the focus of the Community's efforts were primarily: 1) Communist political activities; and 2) military capability and plans. The dramatic changes in Eastern Europe and the Soviet Union have altered that focus, perhaps forever. While the world has not returned to the "pre-apple" Garden of Eden, the continuing military threat we and others face is far different than that of a decade ago.

The United States is now the only military superpower and is likely to remain far stronger, militarily, than any other country. Yet while we are first, and far ahead in the military race, we can no longer claim to be the unchallenged leader in the race for economic supremacy. In adjusting to our New World, it is important to remember that the Soviet Union did not collapse as the result of a weakened military or the threat of opposing military might, but from a failed internal economy, fueled by the technology of communications and the ideology of freedom. The presence of Western military might and the nuclear umbrella may well have been "necessary" conditions, but they were by no means "sufficient". The Soviet Union collapsed despite the fact it had a strong military, if not at least in part as a result of the unbalanced governmental attention to military needs. One of the lessons of the decade is a reminder that true national security rests on a strong economic foundation, not mere military might.

It has been apparent for some time that international economic competition poses a threat to our domestic welfare that is perhaps as great as any threat posed by the Soviet Union in the past 25 years. The present threat requires that we explore how we can now be as effective in providing intelligence support for economic competitiveness as we have been in the past in providing that support for military competitiveness.

The growing awareness of the changing economic environment is evident in public discussions about the role of the intelligence community in collection, analysis

and dissemination of economic intelligence. The extent of that discussion has increased significantly during the past year and there are indications that significant change in the role of the intelligence community may lie ahead. Director Gates consistently voiced his view that the CIA should have a very limited role in the sphere of economic intelligence. Director Woolsey said in his confirmation hearings that he had an open mind and suggested this Administration might be more receptive to expanded intelligence activity to support our international economic competitiveness. The Senate Select Committee on Intelligence continues to hold hearings on intelligence reorganization and a possible re-alignment of the balance between military, political and economic intelligence.

The discussions of the role of intelligence and economic competitiveness often raise significant concerns from many quarters. Much of that concern stems from a fundamental failure to distinguish between economic intelligence activities which, properly understood, should not be very controversial, and industrial espionage, a concept that justifiably provokes immediate, and often heated, criticism.

My purpose today is to try to sharpen the distinction between legitimate economic intelligence and suspect industrial espionage in the hope that a sharper focus will elevate the level of the discussion and perhaps expedite the evolution of one of our most valuable national resources, our intelligence-industrial community.

The significant distinction between industrial espionage and economic intelligence is a distinction that should be well known to all of us, although the distinction is usually thought of in different terms. It is precisely the same as the distinction between clandestine collection on the one hand, and thorough analysis and appropriate dissemination on the other. Today's controversy over economic intelligence is, in many ways, simply an echo of debates that have existed for decades within the community.

Two recent examples will illustrate the point. I returned yesterday from a week of negotiations in Vienna between Austrian and American businessmen who are forming a joint venture to develop state-of-the-art lithography. One of the participants, an engineer who is the president of a semiconductor manufacturing machine company, related an experience which highlights the limited ability of our present intelligence structure to support our national effort to enhance our international economic competitiveness.

This engineer's work requires him to stay abreast of technical developments abroad, including developments reported in two periodicals, NIKKEI Microelectronics and Semiconductor World, that are only published in Japanese. Translation of a single article costs his compa-

(continued on page 11)

(continued from page 10)

ny as much as \$600. This necessary cost of doing business may seem a small factor in his competition with the Japanese manufacturers, but it is a totally unnecessary cost that could be virtually eliminated if we took a proactive view of the role of the intelligence community in economic matters.

Those two periodicals are in fact routinely translated and disseminated in English by the intelligence community, but in classified form. It is hard to think of a valid reason why a government translation of a publicly-available magazine should be restricted to classified channels rather than made available to any American willing to pay appropriate reproduction and royalty charges. By simply expanding our concept of the appropriate consumer for this intelligence product, we would take an important step in the direction of sound economic intelligence policy.

At the other end of the spectrum is the recent publicity about the industrial espionage activity of the DGSE. Their reported activities of bugging hotel rooms, looking through business executive's trash and obtaining secret documents relating to our GATT negotiation positions have led many to urge that we not follow the French lead and that we should instead erect strong walls between the intelligence agencies and the business community.

These two examples demonstrate that the issues raised by clandestine collection are far different than those raised by analysis and dissemination. But those issues are not really new ones. They have been addressed in the past and resolved in ways that suggest we can properly apply intelligence skills to economic issues as well as politico-military matters.

The Intelligence Community has in fact been producing and disseminating economic forecasts for quite some time. The annual USSR GNP estimates were a baseline against which much of the government's projections of military strength and plans was measured. Over the years that forecast moved from the classified to the public arena, thereby providing private sector planners with additional information for evaluating their own interest in the developing Soviet marketplace.

Unlike the situation with respect to technological intelligence, which is in fact widely disseminated through the private sector through the Defense Industrial Security Program, much of the most significant economic intelligence fails to reach important domestic consumers. A good example of this limitation is the continued classification of overhead photography products. While pictures from LANDSAT, EOSAT and other U.S. satellites have been publicly released, we still follow a policy of essentially "no release" of our most detailed, and therefore most useful, overhead photography. Whatever the merits of this policy from a "protection of secrets" perspective, that policy has had the effect both of denying Americans access to a substantial source of valuable information, as well as adversely affecting the balance of trade by giving the French a far less competitive marketplace for their own SPOT satellite products. Our present policy of non-disclosure has

necessarily limited our own ability to utilize overhead products for maximum national advantage. That example should not be repeated; we must find a way of making the finished products of our new economic intelligence more readily available to the non-defense business community so that we can collectively enhance the ability of our business community to compete in the brave new world of a truly international economy.

On the collection side, economic information is both substantially similar and significantly different from collection of military or political information. Both categories of information include a large amount of publicly-available material, while the most significant information, to an intelligence analyst, may often be closely held within a small circle of key individuals or organizations. Both categories of information are, at least under Western law, protected from unauthorized disclosure. Military secrets are protected by systems of classification and criminal law; economic intelligence is often protected by contract, the law of trade secrets and certain statutes. Both categories contain similar subsets of information of significance to the analyst: "hard facts" and "intentions." Acquisition of the closely-held non-public information in both subsets is essential to any truly informed intelligence estimates.

The most significant difference between economic and politico-military information is not the nature of the information, but the character of the institutions and individuals who hold the most significant non-public information. Politico-military information is, by necessity, held by governments and government employees. Economic information, at least in capitalist economies, is more often held by private companies and individuals than by governments. Equally significant is the fact that while the intelligence community knows what's going on within our own governmental and military structures, it has virtually no information on the economic facts and plans of our domestic business sector. In fact intelligence agencies probably know more about the private plans of Japanese businesses than those of American companies. These differences in the character of the holder and the comparative knowledge of domestic and foreign activities presents a fundamental point of departure in any discussion of the role of our Intelligence Community in collecting and analyzing economic intelligence.

Our society long ago rejected the concept that "gentlemen do not read one another's mail" when it came to international politico-military matters. Although the rules of diplomacy and the laws of many nations ban espionage, the unspoken "rules of the game" in practice are that the United States and every other major power knowingly engage in espionage, often against "friendly" as well as "hostile" foreign powers. The sanctions for this activity are, in practice, mild indeed, at least for the professional spies operating under the protection of diplomatic immunity. Thus while our nominal legal structure forbids others from spying on us, while authorizing us to spy on them, the reality is that all parties

(continued on page 22)

Economic Espionage For The Private Sector: You Can't Get There From Here

By: Randall M. Fort

For the past couple of years, the headlines on the issue of economic espionage have been tantalizing: "Security Agency Debates New Role: Economic Spying" (*New York Times*, June 18, 1990); "Should the CIA Start Spying for Corporate America?" (*Business Week*, October 14, 1991); "Some Urge CIA to Go Further in Gathering Economic Intelligence" (*Wall Street Journal*, August 4, 1992); and "Next for the CIA: Business Spying?" (*Time*, February 22, 1993). These headlines reflect the considerable debate which has occurred on the issue of whether the U.S. Intelligence Community should provide direct intelligence support to the U.S. private sector.

The genesis for much of this debate has been concern over the alleged decline in American economic competitiveness and the need to do something about it. Ostensibly, conducting economic espionage against foreign trade and business competitors in support of the U.S. private sector would "help" our competitiveness. In addition, with the end of the Cold War, U.S. intelligence needs to refocus its efforts and resources, and it has been suggested that supporting economic competitiveness could be defined as a new intelligence requirement. It all sounds like a good idea, right? Wrong. For reasons of practicality, utility, legality, and morality, asking the U.S. Intelligence Community to conduct economic espionage on behalf of American companies would most decidedly be a bad idea.

Definitions. There is considerable misunderstanding about the issue, and part of it stems from a confusion over terminology. "Economic espionage," "industrial espionage," "commercial spying," and other such descriptions may or may not refer to the same thing, but are frequently used interchangeably. This paper will use the formulation "economic espionage," which is defined as the clandestine acquisition of economic, financial, trade, and/or proprietary information by an official intelligence service using intelligence sources and methods. Further, the issue under consideration here is not whether such intelligence should be collected at all, but rather whether it should be provided by the U.S. Intelligence Community to the private sector.

What is economic intelligence? An additional point of confusion arises from a misunderstanding of the appropriate role of economic intelligence compared to other intelligence functions. And so to first principles: there is an historic and legitimate role for economic intelligence in support of government policy making. Although economic policy has become a more visible, priority issue of late, it has been an important area of intelligence collection and analysis for many years.



The Intelligence Community (IC) has been active traditionally in three key areas: First, the IC has provided support to government officials as they have made economic policy. This support has included analysis of bilateral and multilateral economic negotiations, identification of economic trends and understanding the intentions of economic competitors, integration of vast amounts of disparate data to present a complete picture of the economic and political factors affecting international stability, and helping policy makers understand the "rules of the economic game" as it is played by others, e.g., to monitor foreign subsidies, lobbying, bribes, import restraints, etc. The Treasury Department, U.S. Trade Representative, State Department, National Security Council, and Commerce Department have all benefited considerably over the years from such support.

A second area of activity for the IC has been to monitor trends overseas in technology that could affect U.S. national security. Our government needs to be aware of foreign developments in computers, semiconductors, telecommunications and the like, which might have impacts on our military capabilities or national security interest.

The third area of IC responsibility is economic counterintelligence (CI), that is, the identification and neutralization of foreign intelligence services spying on U.S. citizens or companies and stealing information and/or technology for use within their own country. With recent revelations of spying by the French and Israeli intelligence services against U.S. companies, the issue of foreign intelligence collection against American economic interests has seized our attention. It is not, however, a new issue.

Remember the KGB? Throughout the Cold War, economic information was a major target for the Soviet KGB and their Warsaw Pact minions. In fact, the KGB dedicated significant resources to the collection of economic information—Line T from the old KGB organization chart was responsible for acquiring scientific and technical information. Additionally, the massive Soviet SIGINT site at Lourdes, Cuba gave them unique and in-depth access to a wide spectrum of U.S. commercial communications. To be sure, the Soviets were interested principally in technology or information relevant to building or countering weapons systems. But not in every case—previous reports have described how the Soviets used communications intercepts to negotiate very favorable terms with U.S. companies on large wheat purchases in the early 1970s.

Since economic information was one of the things our

(continued on page 13)

(continued from page 12)

Cold War adversaries were trying to steal, it was also one of the things our counterintelligence services were organized to try to protect. For example, for 20 years the FBI has run a program called "Developing Espionage and Counterintelligence Awareness (DECA)," which provides briefings and information to American companies, particularly defense contractors, about hostile intelligence threats and activities. In the post-Cold War world, defending against foreign intelligence threats, whether against U.S. military secrets or proprietary economic data, remains a legitimate national security interest.

Intelligence already supports the private sector—sort of. Support for U.S. business has been and remains an important policy priority for the U.S. government. In December 1991, then Deputy Secretary of State Lawrence Eagleburger stated "U.S. competitiveness in the global economy must become one of the pillars of U.S. foreign policy and of our projection of strength and influence." More recently, Secretary of State Warren Christopher declared in a speech last month that one of the first pillars of foreign policy is that it serve the economic needs of the U.S. As the government makes policy in support of U.S. competitiveness, it will be supported in part with information and analysis provided by the Intelligence Community. American businesses are, therefore, the indirect beneficiaries of that intelligence support, since the policies are being made on the private sector's behalf.

The U.S. Intelligence Community is not, therefore, new to the issue of economic intelligence, either the collection of such information for official government requirements, or the prevention of such collection by foreign intelligence services. Further, economic issues are and will remain a foreign policy priority and therefore will be the focus of considerable activity by the Intelligence Community in order to provide support to U.S. government officials.

A new "threat?" What is new is the suggestion by some that intelligence resources should be used in an entirely different way, to provide direct support to the U.S. private sector. This idea is sometimes justified by an attempt to define the various economic challenges as new "national security threats" worthy of treatment by traditional national security tools, such as intelligence support. One of the leading proponents of this view has been former Director of Central Intelligence Stansfield Turner. In an article in the Fall 1991 edition of *Foreign Affairs* entitled "Intelligence for a New World Order," Adm. Turner stated: "...the preeminent threat to U.S. national security now lies in the economic sphere...We must, then, redefine 'national security' by assigning economic strength greater prominence....If economic strength should now be recognized as a vital component of national security, parallel with military power, why should America be concerned about stealing and employing economic secrets?"

"America should be concerned" because such an effort directly on behalf of the private sector would do little to improve U.S. economic competitiveness and would quite likely cause great harm to other important equities. Before looking at the costs and benefits of such a program, however, it is important to address the notion that economic competitiveness should be redefined as a national security threat.

Redefinition fallacy. That the American economy has suffered from a number of economic problems and dislocations in recent years is clear. Many of them, however, are of our own making. The immense and all but uncontrollable budget deficit, with all its impacts on interest rates, availability of investment capital, etc. is 100% "Made in the USA." Low savings rates, onerous regulations, tax burdens, etc. are contributing "non-foreign" factors. To be sure, some of our economic problems are the result of pressures from and actions by foreign countries, but those factors vary widely, from unfair trading practices to simply building better, cheaper products.

Regardless of the provenance of these problems, it is pernicious to define them as "threats," especially "national security threats." They are more correctly labeled as economic "challenges"—obstacles that can be overcome if we follow sound economic, financial, trading, diplomatic, and business policies and practices. A "threat" is appropriately defined as something that can cause demonstrable physical harm: a national security threat is, therefore, something that can cause tangible, physical harm or destruction to the United States. For example, the existence of tens of thousands of Soviet nuclear weapons posed a considerable "threat" to U.S. national security. Thought of in another way, carrying out a "threat" implies a zero sum game at best—one side winning means the other side would have to lose. In the worst case national security threat scenario—a nuclear war—no participant could expect to win much.

Economics is not war. Economic competition, however, is fundamentally different. It is, first and foremost, not a zero sum game. There are winners and losers, certainly, but the gains and losses transcend national boundaries. If Honda of Japan makes an excellent car and sells a large number of them in the U.S., then Honda is a winner and American car companies that lost those sales are losers. But the interactions are more complicated than that. For one thing, American consumers who buy those excellent cars of a type and quality not produced in the U.S. are clear winners. American auto parts companies that sell to Honda are winners, and American companies that produce and broadcast Honda advertisements are also winners. Further, increased market share for Honda, among other reasons, led to their building production plants in the U.S., which is clearly to the economic advantage of the American workers employed in those plants, not to mention the increased tax revenues available to the local jurisdictions

(continued on page 25)

Economic Implications Of Information Systems Security Failures

by Daniel J. Ryan

INTRODUCTION

On August 23, 1992, Hurricane Andrew unleashed 120 mph winds on South Florida, with devastating results. Eighteen schools were destroyed. One hundred and fifty public housing buildings suffered severe damage. Thirty-one libraries had to be closed. Forty fire stations were ruined. Eighty-seven thousand homes were significantly damaged or beyond repair, and over one billion dollars in crops and livestock were lost. The hurricane then crossed the Gulf of Mexico and struck Louisiana with less but still damaging force. It will take an estimated three to five years to rebuild, and the total bill will cost somewhere between thirty and forty billion dollars. Since the United States has the largest economy in the world, Hurricane Andrew was not a knockout blow, or even a crippling one — but it hurt. A larger disaster, one that did permanent or at least long-lasting damage to the economy, could reach the level of concern for the Nation's economic security. A larger storm, a high Richter-scale earthquake in a densely populated area, or a failure of information systems security could produce such a calamity.

INFORMATION SYSTEMS SECURITY

Information systems security is the discipline which protects the confidentiality, integrity and availability of information and the computers, systems and networks that create, process, store and communicate information. The need for protection of the confidentiality of military and diplomatic information or of information that is privileged, proprietary, or private is understood by most people. Computers are designed, implemented and operated to assure that only authorized people can gain access to confidential data. Communications networks use powerful cryptography to ensure that only the intended recipients of messages can read them.

The need to protect the integrity of information is equally important, even when confidentiality is not an issue. Information that cannot be trusted is worse than useless — it costs money and time to create and store, but provides no benefit. A data base that is only slightly tainted may require extensive resources to correct and validate, if it is possible to recover at all. Similarly, information which is not available when required is of no use, even if its confidentiality is secure and its integrity intact. Systems and networks which are not on-line when needed not only represent a waste of the money they cost, the people and companies which depend on them may be irreparably damaged by operational shutdowns or loss of revenue.

Thus, information systems security has both direct and indirect economic consequences. It costs money, time and other resources to protect information and systems, but there are real and significant costs if we fail to adequately provide that protection and loss of confidentiality, integrity or availability results. Because we are highly dependent on information and the ability to readily retrieve, process, analyze and communicate it, we are highly vulnerable to its misuse, corruption or loss. Fortunately, we have not yet experienced a catastrophic single failure of information security with economic consequences comparable to those of Hurricane Andrew, but it is useful and enlightening to extrapolate potential damage both from the failures that have occurred and from the known economic consequences of closely related failures of systems reliability. In extreme — but not so improbable — cases, analysis shows that the economic consequences of failure to protect information could approach or even exceed the amount of damage caused by Hurricane Andrew, directly effecting the well-being and security of the Nation. Conversely, by assuring integrity and availability, and confidentiality where appropriate, we can provide a real competitive advantage to our Country's commerce in addition to protecting the interests and assets of Government and industry in the form of information and the information systems that are expensive to create and maintain and which represent a significant infrastructure investment.

CONSEQUENCES OF FAILURE TO MAINTAIN CONFIDENTIALITY

Some information is meant to be available to everyone. Journalists, publishers, librarians and others spend their careers providing public access to a variety of data, news, fiction, and other sorts of information. But some information is intended to be shared only with a selected audience. Such information might be of a personal nature - information that is not considered to be of wide interest, or which might, perhaps, be embarrassing if generally known. Still other information could be dangerous to the person or group who owns it if it were widely distributed. Such information includes business information that might be used by competitors to the detriment of the company or organization to which the information applies. "Privileged" information, like that between doctors and their patients or attorneys and their clients, is protected in order to encourage free and open communications within protected circles. The national security and law enforcement communities protect the identities of agents or confidential sources of information. And, of course, military and diplomatic

(continued from page 14)

information — so called national security information — is carefully protected in the national interest.

Disclosure of some sensitive information might result in embarrassment or inconvenience. At the other extreme, disclosure of classified information could have serious detrimental consequences for delicate diplomatic negotiations, markedly degrade the effectiveness of expensive high-technology surveillance or weapons systems, or impair the success of military operations. For each of these cases, and at every point in between, there are potentially significant economic consequences of failure to protect the confidentiality of information. In some of the worst possible cases, our high-technology surveillance and reconnaissance systems could be rendered useless — or worse, misleading — if their capabilities and limitations were known. Billions of dollars would have been wasted on their development, bad decisions made based on tainted information they gathered, and invaluable lives of U. S. personnel needlessly lost.

As the Cold War and the threat of nuclear confrontation fades, technological and economic intelligence take on increasing importance. While the Commonwealth of Independent States remains a region of great concern, there is increasing awareness of the dangers inherent in technology transfer to third world nations and the proliferation of nuclear, chemical and biological weapons and associated delivery systems. Thus, compromise of information developed in this Country and by our allies that permits us to build and operate highly accurate weapons, such as those used in the Gulf War, and weapons of mass destruction is of great concern. Knowledge about our smart-weapons systems could result in their being avoided or met with effective countermeasures, so that billions of dollars in development, production and operations costs would have been spent for no gain, and battles or wars lost. On the commercial front, loss of confidential information concerning financial and trade issues or proprietary technological developments of commercial importance could harm our Country by reducing our competitive edge. Information about environmental conditions and natural resources may also need protection.

The threat comes not just from our former enemies, but in many cases from our erstwhile friends. The French intelligence service Direction Generale de la Securite Extérieure (DSGE) has been found using the traditional espionage techniques originally developed to spy on the Soviet bloc to obtain trade secrets from foreign business executives traveling to and in France. Trade secrets so garnered have been passed to French industrial firms which have used them to vie successfully for competitive awards. Other foreign intelligence services have also mounted operations aimed at obtaining U. S. technology secrets. Techniques employed range from intercepting fax, voice and telex communications to bugging hotel rooms and aircraft seats, from stealing a company's trash to bribing its employees.

Failure to protect the confidentiality of our information assets can easily mount to staggering sums. Opportunities and contracts lost to foreign competitors mean lost revenues, worsening trade balances, increasing unemployment, and a declining standard of living.

CONSEQUENCES OF FAILURE TO MAINTAIN INTEGRITY

While the economic consequences of loss of confidentiality may be severe, loss of information or degradation of its value may be even more catastrophic. In 1985, a New York bank had software problems that resulted in modifications to its transaction records. To cover its accounts while it diagnosed and corrected the problem, the bank had to borrow over \$23 million, at a cost of \$5.6 million in interest. Loss of the integrity of data bases, software, and systems in all sectors of the economy can have both economic and safety consequences. Consider that the air traffic control system, stock transactions, financial records, currency exchanges, Internet communications, telephone switching, credit records, credit card transactions, management information systems, office automation systems, the space program, the railroad system, hospital systems that monitor patients and dispense drugs, manufacturing process control systems, newspapers and publishing, the insurance industry, power distribution and utilities all depend on computers. The law enforcement community also relies heavily on the integrity of information and information processing systems.

Integrity of information can be threatened by a variety of means, including physical destruction of the systems that create, process and communicate information, or destruction or erasure of the media containing the information. Destructive programs called "logic bombs" may be placed in data processing systems and networks where they lie in wait for either a specified set of conditions or the passage of a specified length of time. Then they wake up and destroy the information in the computer or its data storage peripherals. Take, for example, the case of a young programmer who placed a logic bomb in his company's personnel system. The malicious program checked periodically to see if his name was still on the list of employees. When he was fired, his name was removed from the list and the logic bomb destroyed the company's personnel records. In another case, on April 11, 1980, many IBM 4341 main-frame computers shut down due to a logic bomb that had been planted by an unhappy employee. In yet another instance, a medical center lost nearly 40% of its data to malicious software.

Computer viruses may also destroy data. The news media has widely reported the discovery of the Michelangelo virus, a time bomb set to go off on March 6 (Michelangelo's birthday) of any year and destroy the contents of a personal computer's hard disk. Thousands of viruses are known, many of which destroy data, and

(continued on page 24)

(continued from page 3)

sense, but they should be made because we no longer need these programs—not because we have to protect intelligence community manpower.

The Partnership is Broken

In the past, a partnership between the administration, congress and industry formed to support the National Reconnaissance Program. It was above partisan politics, within the Intelligence Community, within the executive branch of government as well as between the executive and legislative branches. Most surprisingly, NRO programs were also immune from the normal day-to-day politics of the Congress and their concern for “constituent issues.” The reason for this comity between the various players was the critical nature of the subject. The satellite program was just too important to the nation to let the “normal” actions of government and bureaucracies take their toll.

I began this discussion with the question, “how important is satellite reconnaissance to the Nation?” I believe the answer is that satellite collection is the foundation of our Intelligence Community, the basic sensor abilities of our Nation that only the committed actions of concerned members of our government can sustain.

But agreement reached on the premise that this function is critical and the individual commitment of the various players is not enough. From the perspective of industry, the partnership between the NRO and industry is broken as well. In the past the government was able to decide what programs they wanted; Congress provided the funding; and there was little wasted motion or wasted resources on either side. Today, the “word” of the NRO is no longer honored in industry. Programs start, stop and sometimes start and stop several times. This wastes both company and government resources plus makes the NRO look more like a normal bureaucratic organization. The unfortunate result is that the trust that existed for so long between the NRO and the contractor community that supported it is broken.

Brutal Honesty is Needed

A continuing dialogue between the administration, Congress, the NRO and their contractor base is essential. What we need is brutal honesty. The contractor world has a difficult job in balancing their historical commitment to this program while managing profitable businesses. It would be very helpful to the contractor world if the administration, the Intelligence Community and the program shared more specifics on the reality of the situation today. For example:

- * Budget—The budget is going down; we know that. The NRO needs to tell people realistically what is being spent on which budget categories and how these percentages are likely to change. Most of us in industry and the Intelligence Community want to hear that the other guy’s budget is going down, not ours.

Generalities here are not helpful; specifics would be.

- * Design to cost—For the foreseeable future, the reality is that all initiatives will be budget constrained. In this context, we would save everybody much time and effort if we admitted that new initiatives are design to cost exercises. To do this, however, the administration needs to tell industry what the budget constraints are.

- * Clearly communicate priorities—The NRO needs to galvanize its troops in a way that everybody is working to the same set of priorities, not their individual agendas. The only way this can happen is if we all understand what the priorities are, and that can only come from the executive branch of government.

What’s the Competitive Advantage?

The Intelligence Community needs to develop a strategic plan that identifies the top level requirements of the future and then describe the core programs and activities needed to satisfy these requirements. Then, the NRO needs to determine and articulate the competitive advantage of satellite collection. In industry, strategic plans that do not articulate and capitalize on the competitive advantage of the organization are failures. It is a fact that intelligence collected by satellites compete with other forms of intelligence collection, many of which claim they can do “the job” cheaper and maybe better.

The clear competitive advantage of the past (only satellites can penetrate the “closed societies”) is gone. The most important contribution the NRO can make to the future is to crisply and simply articulate the competitive advantages (and disadvantages) satellites have as compared to other forms of collection. In industry this is usually simple and boils down to one of two fundamental strategies.

- * You have a unique product that everybody wants.

- * You have the best value product on the market. That is, the product that has (in the customer’s eyes) the highest quality for the most reasonable (not always the lowest) price.

For a long time, the NRO neatly fit into the first strategy. It provided a product that was unique, could not be obtained any other way, and people were willing to pay to get it. Now we have to recognize that the NRP actually fits into the second strategy, which is much harder to articulate. The issue is, can the President of the U.S. be adequately informed on the state of the world without the truly unique capabilities of satellite reconnaissance? How do you determine the value of that one critical piece of information that prevents hostilities, or saves the lives of U.S. servicemen or women, or aids the Administration in an important trade negotiation?

Together—Congress, the administration, the NRO and industry—must stand up to the challenges we all face in trying to reinvent the NRO for the future—how

(continued on page 17)

we review the requirements, develop programs and deliver a product to the ultimate consumers of intelligence—policy makers, decision makers and military commanders. We must reinvent the program for the future. The original program was invented in 1958 because of a problem that no longer exists. It developed capabilities many of which are no longer perceived as being important. Yet, satellites are needed for the global uncertainties we will certainly have to deal with in the future.

Birthplace of Technology

Because of the heavy security concerns that have traditionally enshrouded all aspects of the National Reconnaissance Program, very little has been shared regarding the contribution made by these programs to the U.S.'s overall competitive advantage in space technology. NRO programs have been the technological engine that has fueled the unmanned space business. It is an important issue in that we are dealing with a national technological treasure that is vital to our industrial base and the nation's future competitive posture in the space industry.

A few examples of the contribution of NRO programs to space technology follow.

Essential to the design of any spacecraft is the integration of space "deployables," for example, where a satellite extends a boom with an antenna for communications or a solar deployment to provide energy to the satellite. Space deployables found their origins in NRO programs.

How a vehicle moves through space and how we control a complicated and flexible body is a difficult challenge. This challenge was first met by NRO programs. So, too, was the advanced development of a variety of space structures, the use of advanced materials, wide-band data links and the use of GaAs chips.

While other federal agencies funded large optics research in the past (DoD, SDIO, NASA, DARPA); today only the NRO has a continuing interest in this technology. Without the NRO, this technology would be extinct in the U.S.

The NRO has been a birthplace of unmanned space technology. Before the United States gives up on yet another high tech industry, the decision makers need to consider this aspect of the NRO's vital technological contribution to this Nation.

Conclusion

Satellite reconnaissance is still required. Congress and industry for the last three years have recognized, however, that dramatic changes in the world require equally dramatic changes in the satellite reconnaissance program.

A new vision for the NRO has not emerged. The result is that no road map to the future has been agreed

to. In part, this is due to bureaucratic inertia and too many competing interests, all striving to protect their piece of the diminishing pie. More important, because of the difficulty in articulating a realistic assessment of the threat to U.S. vital interests, after the fall of the Soviet Union and Warsaw Pact, the NRO has not been able to move forward with new development programs to deal with the future. We do need future systems, but

- * fewer of them which are designed to cost,
- * that meet the requirements of decision makers, and
- * support military operations.

Everyone in industry realizes that there will be fewer players in the future. Instead of stringing along a lot of companies, down select now. There is no single act that the government could take that would help the "industrial base" issue more quickly than making the programmatic decisions needed and then sticking with those decisions. Continued delay and indecision is, in fact, a decision to destroy the NRO's industrial base.

Critical Technologies and Skills Must be Maintained

A careful distinction must be made between industry conversion and industry maintenance. Some critical technologies may be converted to commercial ventures and should be nurtured to keep our nation competitive in the space industry. Just as important, however, are the few truly unique technologies that are only applicable to the space reconnaissance business. These unique technologies will not, repeat not, be protected within the parameters of defense conversion or within the industrial base of the defense industry. They are unique to satellite reconnaissance. If they are lost, the Nation's ability to conduct satellite reconnaissance will be severely harmed. Reconstituting these technologies and skills (unique to satellite reconnaissance) will not only be expensive but could take years. What is more dangerous is that they are in the process of being lost while they are still needed.

The survival of the Satellite Reconnaissance industry in the United States is at risk.

* The industry has far more capacity than is required by future national security requirements; too many companies are competing for too few programs.

* The past administration continued the old practices of spreading the work among a variety of companies, none of which have a large enough business base to sustain this effort.

* Current programs continue in production with less and less new engineering content. The industry is losing its ability to design and develop new systems. These critical engineering skills are exiting the industry.

Many of the current critics of the NRO will say-*so what?* Industries come and go. The contractors that have supported the NRO have had one "hell of a ride" for 25 plus years. Why should you be immune? And, in

(continued on page 21)

Colloquy, May 1993

and how it could be tailored for Army shelters and "Army unique" intelligence support at a fraction of the time and cost of developing an all new ASAS-II. There are many such examples of similar situations, some within a single Service.

Budget cuts to intelligence are a reality that many have yet to accept. The government tendency to protect personnel and existing programs and bring more work in-house will not survive. Bold or perhaps radical thinking is necessary with major impacts on national and tactical intelligence systems architecture, programs, and personnel to be expected.

For the SMO mission, the watch words are joint, real-time operations using precision strike munitions. Therefore, the TIARA (and NFIP) must consolidate and develop joint solutions for intelligence support (or better yet call it real-time combat information) and break down the still existing barriers between operations and intelligence in SMO.

Programmatically, the TIARA account must be brought under more centralized oversight and control by the ASD(C³I) to avoid situations like the CARS and ASAS stories and the on-going saga of tactical imagery processing and dissemination between JSIPS, CARS, and other solutions.

The requirements to support precision strike operations, advanced land combat, special forces, specialized naval operations, and ballistic missile defense are rapidly emerging and in many cases are driving new and very different intelligence requirements for both NFIP and TIARA systems.

The biggest SMO budget and programmatic challenge facing the DCI and SECDEF is the degree to which the NFIP will (or will not) restructure to meet rapidly evolving military technology imperatives, doctrine, and tactics.

ISSUE III:

TECHNOLOGY IMPERATIVES AND THEIR IMPACT ON INTELLIGENCE

The development and application of technologies which have an impact on intelligence collection, processing, and reporting in both defense and non-defense sectors, is occurring so rapidly that the Intelligence Community is hard-pressed to keep up. The consequences of technological obsolescence are potentially serious in SMO, in technical intelligence collection, and in copying by intelligence organizations with the rising tide of gigabyte per second digital data networks transferring all manner of material of potential intelligence value. This means that the IC must become more technologically nimble and able to rapidly shuck old systems, techniques, and personnel.

To illustrate this potential technological impact, four technology-driven examples are presented: (1) the dramatic technological development and proliferation of high performance networks and computing, including

on-line mass storage of tens of terabits of data; (2) the SMO requirement to detect, identify, localize and strike (with precision) disparate, mobile, tactical military targets under any weather or time conditions within minutes of first detection; (3) the employment of distributed, seamlessly networked modeling, simulation, and prototyping technologies; and (4) the near-term development of global cellular voice and data systems and pager communications satellites.

TECHNOLOGY IMPERATIVE 1:

HIGH PERFORMANCE NETWORKS, COMPUTING, AND MASS DATA STORAGE

Global communications networks are rapidly evolving into a network of networks often referred to as an internet. In an internet, many different kinds of networks can be connected by sophisticated gateways. To move massive amounts of voice, data, and video signals, the new global approach is called Asynchronous Transfer Mode (ATM) cell switching using a Synchronous Optical Network (SONET). The ATM technology provides efficient multiplexing of bursty data traffic with real-time, constant flow traffic and routing within the network using virtual circuits.

The introduction of SONET technology networks permits data rates from about 52 MB/Sec to 2,500 MB/Sec. Such networks will be in place by the year 2000. Couple that with new end-to-end encryption security for multi-level network security and the Intelligence Community has a major challenge.

In the area of computational power and prime performance, the trends are:

Capability	Today	Year 2000
- Microcomputer Systems	100 SPECMARKS for \$20K	1,000 to 10,000 SPECMARKS for \$20K
- High Performance Computer Systems	20 GFLOPS for \$20M	Greater than one TERAFLOP for \$1M
- Memory	4 MDRAM at \$5.00 per MEGABIT	256 MDRAM at \$.08 per MEGABIT

These data can be viewed by the Intelligence Community as both good and bad. The good news is that Intelligence Community components will be able to procure significantly increased computational power at lower cost. The bad news is that so can the bad guys. Global proliferation of computer and communications technology is a major concern to intelligence.

Finally, in the technology of massive data storage, there are systems under development today to intelligently store on-line tens (50 to 100) of terabytes of data and to be able to retrieve data out of that database in tens of seconds. Data input rates of gigabytes per second are contemplated.

(continued on page 19)

These technologies are all unclassified and are being developed on a global scale to global standards and protocols to ensure network interoperability and equipment standards. The rapid introduction of ATM cell switching over Broadband Integrated Service Digital Networks (B-ISDN) presents a formidable challenge to intelligence.

TECHNOLOGY IMPERATIVE 2:

PRECISION STRIKE

The national and tactical intelligence communities are now being asked to develop the capability to support, in near real-time, the detection, identification, and localization (to within a few feet CEP) of mobile or moveable tactical military targets. These critical mobile targets (CMT) could be surface-to-surface missiles (SSMs), command and control centers, tactical aircraft, surface-to-air missile (SAM) sites or naval vessels, just to cite a few examples. Since U.S. forces could be deployed virtually anywhere, the required intelligence assets must have global access. Further, response time to a crisis may be measured in hours, in which case deployment of tactical collection assets such as the TR-1, River Joint, EP-3s or JSTARS cannot be depended upon in terms of time or necessary target access. All-weather and nighttime operations are required.

The stress is on very timely (minutes not hours) intelligence response in providing the targeting intelligence to the operational forces. This not only implies radically improved collection processing, but also the need for diverse communications links, which in some cases are linked directly to airborne strike platforms (e.g., an F-15E, F/A-18 or B-1B) or to ground based, deep strike systems such as ATACMS. The Intelligence product could be imagery or SIGINT, or a correlated product of the two, in time and event location. Moving target indication (MTI) would also be essential, as demonstrated by JSTARS in Desert Storm.

Today, the national Intelligence Community is (except in very limited ad hoc operations) not structured to meet precision strike requirements. The DARPA program known as WARBREAKER is developing high fidelity simulations of such systems concepts to evaluate which can be accomplished and how well it would work. This includes simulation of national systems played into realistic tactical scenarios.

In my people's judgement, the issue is not necessarily the technology to redesign the NFIP systems into near real-time precision strike support. Significant studies and developments have been made in several technical areas which could lead to such capabilities. The real issue is whether the bureaucracies which control the NFIP capabilities will step up to this new challenge in a joint, integrated way.

Creation of new entities such as the recently established Central Imagery Office (CIO)** is hardly the response the Services need, even though the CIO is designated as a "Combat Support Agency" and all that implies. The CIO operates under directives issued separately by the DCI and the Secretary of Defense which reflect management and operational compromises, as is evidenced by the fact that separate directives were con-

sidered necessary. The result is an emphasis of national intelligence requirements rather than on what is needed for support to military operations. With DoD the overwhelming consumer of imagery, logic would seem to say that all tactical and national imagery requirements, systems architecture and control, and dissemination should rest in DoD. Such is not the case today.

Furthermore, the creation of a CIO continues the separate stovepiping of imagery and SIGINT. These two "ints" need to work requirements jointly and a mechanism needs to be put in place to determine which "ints" or combination can best satisfy a requirement. To illustrate how difficult this will be, the head of the prior (to CIO) imagery requirements office once spoke at a classified meeting for over thirty minutes on imagery requirements and never once even mentioned SIGINT as one alternative or complement to a collection requirement. The plea was for more and more imagery systems to meet "his" requirements.

TECHNOLOGY IMPERATIVE 3:

DISTRIBUTED MODELING AND SIMULATION

This technology imperative is important to the Intelligence Community on two counts: (1) it provides tools and techniques to greatly assist in the concept formulation, requirements analysis, prototyping, simulation, design and manufacturing, and testing of technically complex systems; and (2) using this technology, an adversary can more rapidly develop significant weapon system capabilities, evaluate and test them using simulation and modeling, rapidly develop a few prototypes that could be useful in crisis, and accomplish all of this within the confine of small, obscure facilities which would be very difficult to detect and penetrate.

This development process would be much more difficult to detect using technical intelligence means and could result in technological surprise. The U.S. took prototype systems (such as JSTARS) to war in Desert Storm to great effect and it should be expected that potential adversaries could do likewise in the future.

To date, my impression is that the Intelligence Community has neither employed distributed modeling and simulation***in their systems acquisition process to any large extent, nor have they seemed to worry very much where this rapidly developing technology is being employed in target countries. The technology is all unclassified and the enabling technologies are available outside the U.S.

The Intelligence Community components could potentially save money and improve their acquisition processes if they turned to modeling and simulation technology more aggressively. The DoD has established a Defense Modeling and Simulation Office (DMSO) which has funding to assist in modeling and simulation initiatives. Also, DARPA spends about \$40 million per year on this technology. During the recent DSB Summer Study on Modeling, Simulation and Prototyping, the Intelligence Community was conspicuous by its absence from any participation, briefings or apparent interest.

(continued on page 20)

TECHNOLOGY IMPERATIVE 4:

THE DEVELOPMENT OF GLOBAL, SPACE-BASED CELLULAR VOICE AND DATA COMMUNICATIONS SYSTEMS, AND SATELLITE BASED PAGER SYSTEMS

There are currently nine (9) different commercial, mobile user satellite communications systems either in-being or in active consideration by the FCC for regulatory approval. This does not include other systems concepts for low earth orbit (LEO), small satellites to create a global pager service. The FCC recently approved a band of frequencies for this pager service.

Several of the new satellite communications system concepts are cellular telephone architectures to provide both voice and data services. System architectures include geosynchronous, high inclined medium earth orbit (MEO) and LEO systems. One LEO concept employs a complex spacecraft with on-board switching and cross-links that would allow a user with a handset to place a call to another user virtually anywhere on the globe without requiring land based facilities to complete it. Other MEO and LEO concepts are simply bent-pipe transponders and would need ground based gateways for control and interconnects to ground based networks.

Another significant feature of these systems is the capability to accurately geolocate and identify all users in real-time.

From a SIGINT collection perspective, these new global cellular systems pose both legal and technical challenges of unusual significance to the Intelligence Community.

ISSUE IV.

THE FREE-FALL IN THE BUDGET AND THE INDUSTRIAL BASE

Despite the obvious continuing challenges to the Intelligence Community for technical modernization, Support to Military Operations (SMO), and an expanding global target base with new collection priorities, there is little doubt that the overall investment in intelligence will continue to decline. Perhaps the decline will be on a somewhat less severe slope than the rest of the defense budget, but probably not by much.

The negotiation of START I and now START II, coupled with the evolving U.S. political and economic relationships with countries formerly part of the Soviet Union, have strongly mitigated the perceived strategic nuclear threat and the threat of large-scale, land combat operations between the countries of NATO and the Warsaw Pact. The remaining potential regional conflict scenarios in which the U.S. might become involved would suggest to many that an even smaller U.S. force structure than the current Base Force would be adequate.

In short, the American people, and especially the Congress, do not see a compelling need to sustain current defense investment levels in competition with domestic programs and intractable budget deficits. As

a result, the prevailing thinking is that domestic political and economic demands will force President Clinton to reduce defense, intelligence, and probably NASA investments well beyond those projected by the former Bush administration's six-year plan for FY-94-99. For the defense industry, the message is quite clear on the budget. The message is less clear, however, as to how the DoD and Intelligence Community plan to assist (if they do at all) industry in coping with the budget reductions. The free-fall policy of the last administration and the suggestions to convert to commercial products were no help at all. Clearly, the industrial base is going to shrink further and more industry consolidations are likely.

Keep in mind that the option to cut budgets by closing or dramatically reducing major DoD laboratories, mod centers, and depots is probably politically unavailable to the Secretary of Defense because of Congressional interests. But, many believe major savings could be achieved by closing these government facilities, while at the same time reducing the direct competition with industry for mod work, R&D, and support services.

The major policy question on industrial base is: Is the industrial complex which designs, builds, and supports the Intelligence Community systems so valuable and fragile that the government must "protect" this industrial base (e.g., find continued high levels of funding for R&D of new technology as a minimum)? Many do not think so for a variety of reasons:

- ~ Components of the skill base needed to design and produce big ticket items, such as reconnaissance spacecraft systems, are very similar to the skills required to produce NASA/NOAA space systems, commercial spacecraft, and some SDIO systems. In fact, the advocates of smaller, less complex space-based reconnaissance systems would argue that an adequate skill base exists and can be sustained at much lower cost than the current NRO approach.

- ~ The skill base to design and produce many, if not all, of the database systems to receive data at hundreds of megabytes per second, smartly archive massive amounts of data, and intelligently and quickly retrieve specific data is largely in either the commercial industry or in NASA-sponsored developments such as EOSDIS. Other sources of this skill base are in the DoD modeling and simulation developments where massive digital database systems are required. Networking with high performance communications is also technology heavily used in modeling and simulation.

- ~ In other specialized skill areas such as high performance ground and airborne SIGINT collection, processing, and reporting systems, the required skills are very similar to those required to design and produce electronic warfare systems and so-called Electronic Support Measures (ESM) systems. In fact, we are seeing a move to deploy very capable ESM (e.g., SIGINT) systems in non-traditional platforms such as JSTARS, AWACS and tactical aircraft using contractors not necessarily employed by the Intelligence Community. For example, a high performance ESM systems with precision direction finding (better than one degree) is in flight test on an F/A-18. This was developed by a contractor that

(continued on page 21)

(continued from page 20)

is not in the airborne Intelligence Community industrial base.

~ Commercial developments in microprocessors, memory devices, communications, computers, and networks are all moving ahead more rapidly than the government can take advantage of them. Further, many, if not most, ground-based intelligence systems can be developed using this commercial off-the-shelf hardware and even software such as database management systems. The government simply does not have to invest in these technology areas or to try and protect the associated skill base.

~ The "issue" raised by some that government non-support for the industrial base will result in significant start-up costs to recreate the base is more likely a boogey-man than a real issue. The circumstances and specifics of the desired capability are influenced by so many factors as to make realistic estimates impossible to compute except on a very specific case-by-case basis. My guess is that nobody has done a skills analysis versus future program requirements to even guess at that skills and technologies are truly "key" and then offer up an affordable and practical plan to retain those skills.

SUMMARY

Dick Kerr raised some excellent points about intelligence and industry which deserve more thoughtful and expanded discussion than presented in this paper. Perhaps the new DCI and SECDEF could create a joint government/industry team to examine these and other issues. Such an effort was recently completed for the Secretary of the Army where many of these same issues are of concern.

The Intelligence Community also needs to perform a more rigorous examination of itself and the way it does business with its customers.

There is a new thrust in commercial industry called "relationship marketing." This approach has the supplier intimately knowing his customer to the point of anticipating his changing needs and responding just in time with a quality product. They have learned that this is the only way to retain and grow business in highly competitive cost and quality-driven markets.

This is perhaps the single most important action the new DCI could take - know your customer, understand or even anticipate his requirements, and become customer-oriented. The core systems and capabilities required to serve the customer could be better defined and defended if you really know your customer. Maybe some customers would even help sell the program to Congress.

*Issue III expands on this point.

**See DoD Directive 5105-56, dated May 6, 1992.

***See the September 1992 Defense Science Board (DSB) "Report on Modeling, Readiness, and Prototyping" for a description of the technology, its applications, and a technology assessment and forecast.

Editor's Note: Mr. Latham is the former Assistant Secretary of Defense C³I (1981-1987). He is currently Corporate Director, C³I Programs, LORAL Corporation.

(continued from page 17)

any event, if we need it later we will simply pay to reconstitute the capability.

The answer from our perspective is that we are not asking for "special" treatment. What we are asking for is simply a decision. What is to be the architecture of the future; what are to be the programs; and what will be the budget? Industry knows how to operate when it knows the game.

The conclusion should be that there is an important role for satellite reconnaissance in the Intelligence Community of the future, and this role needs to be clearly articulated and "bought into" by both the administration and Congress. The currently broken covenant between industry and the NRO will need to be restored if the challenges of the future are to be met with the same creativity and effectiveness as they have been in the past.

Editors Note: Mr. Kohler is the Vice President and General Manager of TRW Avionics and Surveillance Group (ASG)

(continued from page 9)

in international markets, the U.S. vendor base will be more financially capable of supporting the high performance/limited production needs of the U.S. intelligence community.

(6) U.S. diplomacy can be strengthened by the ability to offer to transfer intelligence/security equipment to favored allies to increase their capability to support U.S. regional security objectives. The ability of U.S. diplomats to offer a highly effective means (i.e. American C³I equipment) to address a local/ regional threat can be a basis for eliciting a greater commitment of defense resources by an allied nation in support of U.S. regional security objectives.

(7) By creating a "family" of regional players with effective C³I resources to meet local/regional needs, the U.S. can maintain an integrating role through its national resources with global capabilities.

(8) Aggressive American pursuit of the international intelligence/security market can serve a constructive influence in discouraging and rendering manageable the growth of local/regional disputes. Nations allied to the United States do not necessarily share local or regional interests. American participation in these markets can discourage the growth of exacerbation of regional antagonisms.

Editor's Note: Dr. Schneider is Chairman of Schneider-Sohn & Associates. He previously served as UnderSecretary of State for Security Assistance, Science and Technology (1982-1986).

(continued from page 7)

certainly need to be seen as a strong signal of concern about the pace at which the community is refocusing its activities in light of the end of the Cold War.

The Committee will look to the Director of Central Intelligence to present his vision of where the community ought to be in the mid/late 1990's and to illustrate how his budget in 1994 fits into his overall goals and objectives as he sees them. The Committee has a responsibility to the other 416 members of the House to bring an authorization bill to the floor which recognizes budgetary realities, but also makes the case for the continued necessity of an effective intelligence collection, analysis, and dissemination capability. The intelligence budget, may or may not, be a contributor to the overall deficit reductions. It should not be lost that any reductions made by the committee in the intelligence budget simply contribute, to the amount of money available to the Armed Services Committee budget, and therefore there is no direct effect on deficit reduction on the intelligence alone. It fits into the bigger part of the Armed Services Committee budget. I must be really candid with you. Many of my colleagues have come up to me at this time and they are looking for more and more money to cut and they are saying, 'Can't you contribute, can't intelligence give some more money! My response quite candidly has been I can't do a thing until I see where the Director wants to take the community. At this stage it would be stupid for us to recommend specific cuts until we see where his budget is going.

Now I'm not going to go too much more, except to say that you all represent the voice of this industry. I think that you all at SASA and those of you in industry and of course those of you in the community need to provide to us the information, the input of how to preserve the technical industrial base and improve the overall cost effectiveness in supporting U.S. intelligence. I think your input to us, I'm not saying this to patronize you, your input to us is very, very important particularly as we get into a modern world where there's a lot of technology to share and we have to decide what we can sell and what we can't sell. One of the things we've been talking about has to do with imagery satellites. The world of the next 20 or 30 years will probably see the ability of the private sector to become very astute in the business. We have to sit and talk a little bit about how we allow this to happen. What controls do we put on export of imagery and satellites. What role does the intelligence community have in this context.

This nation is well served by a professional, capable and dedicated intelligence work force. We ought not loose our competitive edge in this very dynamic, challenging and risky business. Vernon Walters, a former SASA Baker Award winner, one of your own, said in his book, *Silent Mission*, 'Intelligence demands immense patience. An operation may be undertaken that will produce almost nothing for a long time. Then suddenly it will yield enormous results that amortize the project many times over. Another will yield nothing.' Sounds a little like politics. 'The application of the principles of cost effectiveness to intelligence demands a very special kind of skill and judgment. We must select our priorities for intelligence carefully and then devote the appro-

priate amount of resources to those priorities. It is clear that intelligence is not really an exact science. Good judgment in dealing with it is as always the most important element.'

His observations mean a lot to me as Chairman of the committee. I believe very strongly that knowledge is power. Information is the key to winning in the business sector, in politics and in the world economic and political community. So we must have that knowledge. We have to have that information. The intelligence community is where we get it. Obviously in a modern world we have more limited budgets. Our choice then is to try to pare those down responsibly, but still keep enough meat so that we don't end up with something that is skeletal and doesn't do any good.

Finally, I would like to reinforce a point I made before because it relates to what you do. If the public doesn't support the program, it will not last. In a democracy that's just the way things are, and you and me and those in the community just can't assume that things will be that way in the future because they've been that way in the past. At the same time I'm telling you that neither I nor my colleagues have in mind in anyway what-soever the decimation of the ability to collect good intelligence about what's happening in the world. We'll only be strong if we have a good, solid, effective intelligence community. And that's what I intend to push for as long as I'm chairman of the committee.

Thank you all very much."

Editor's Note: Congressman Glickman (D) was appointed Chairman of the House Permanent Select Committee on Intelligence on January 1993. He represents the 8th Congressional District in Kansas. The foregoing presentation was made at the SASA Inaugural Distinguished Lecturer Program Dinner on 9 March 1993.

(continued from page 11)

knowingly tolerate substantial espionage activities because all sides believe that, on balance, they have more to gain by a world order of secrecy/spying than by either total availability of information or unrestrained efforts to prevent "hostile intelligence activities."

That somewhat schizophrenic posture toward politico-military intelligence is sharply contrasted to the prevailing public and private sentiment about domestic economic privacy. Contemporary American morality places a high value on preservation of economic privacy, perhaps higher than any other area of privacy. Both personally and institutionally our society guards its economic data against unauthorized intrusion. Proposals for public access to individual tax returns and corporate business plans are not likely to be pressed by any aspiring politician or senior government official.

If the assumption of increasing focus on understanding the economic forces around us is valid, then it is inevitable that our public officials will increasingly demand to have the best and most current information available instantaneously. Having become accustomed to the luxury of KH-II, CNN and Pentagon-to-front line

(continued on page 23)

communications, our leaders in the next century (if not President Clinton) are not likely to be very patient with an inability to forecast significant changes in production runs of Hondas, BMWs and Chevrolets. The policy issues posed by this inevitable demand are substantial: 1) Do we want our government to engage in international economic espionage with the probable result of reciprocal foreign intrusions into the American economy?;

2) How much information about our domestic economic activities are we willing to share with our own Government?; and 3) Do we want to use clandestine means to acquire economic intelligence at home or abroad?

Although dissemination issues are substantially different from collection issues, resolution of the separate issues is in fact closely tied together. Clandestine collection historically breeds classified dissemination. Open-source collection furthers, but does not guarantee, public availability of finished product. If the Intelligence Community were to follow the models of the Departments of Commerce or Agriculture, it would seek some method of confidential reporting of essential data followed by secret government analysis and pre-announced public releases to avoid giving competitive advantages to particular companies. If the Intelligence Community were to follow the DISP model, it would enter into classified relationships with preferred providers of company-sensitive data, analyze the data and provide it in classified form to the community of providers. This model would give preferred treatment to those business who were willing to share their own "secrets" with the government in exchange for access to the products of that process.

It must be recognized that the business community will undoubtedly approach this world of information exchange with great fear and trepidation. Business efforts to keep trade secrets from competitors is a deeply ingrained instinct. Business fear about government access to "hard economic data" and business plans reaches the level of virtual paranoia. Even the most conscientious, law-abiding business executive will shiver if one proposes an "open-files" policy in which the CIA can gain total access to production forecasts, compensation studies, productivity analyses and pricing strategies. Yet without such access to both domestic and foreign company data, we cannot really expect meaningful economic intelligence activities.

The problems posed by involving the intelligence agencies are substantial. Collection and dissemination pose significant policy choices. Analysis has never been the strongest of the intelligence skills and there is no reason to expect that economic forecasting by government professionals will be significantly better than the same tasks performed by the private sector. It is axiomatic that economics remains an art, not a science, and reliability in this area is notoriously limited. Given the scope of the problems presented, it is reasonable to inquire whether there is any role for the government in expanding activities in the arena of economic intelligence.

The American society is deeply rooted in capitalism

and rests on a fundamental mistrust of mixing government and business. While the modern American government is far more entwined in business concerns than was the case a mere 100 years ago, there remains a strong vestigial belief in our society that the wall of separation between government and business should not be that much shorter than the wall between Church and State. That belief, coupled with a laissez-faire foreign trade policy, might lead to the conclusion that the Intelligence Community should stay out of the field entirely, leaving matters of economic intelligence to other federal agencies and the private sector. That result is certainly the easiest solution to the multiple conflicts and adjustments that would be required if we prefer a more active role for the community. That easy path may, however, not be the best in the long run.

Our European and Asian competitors are accustomed to societies in which there is a substantially lower wall between business and government. While their economies are not Marxist, there are far from pure capitalist societies. As the world has shrunk, the role of government as a partner in business has correspondingly grown. It is probably true that it is now impossible for our government to disengage from business, even if either side really wanted a disengagement. The future undoubtedly will continue to require a mixed economy with a probability of increasing role for government because competition in a global market will require our government to become more like those of our foreign competition.

Our plans for the future use of our Intelligence Community assets must be formed in a manner consistent with our anticipation of the future role of government as a participant in the world economy. If, as suggested, that role will increase rather than decrease, it makes little sense to plan for a negligible role for intelligence agencies in collection, analysis and dissemination of economic intelligence. Our fears over how to blend intelligence and business are genuine, but the problems facing us cannot allow those fears to cause us to solve the problems by simply avoiding them.

Our defense industry has developed a close and essentially comfortable working relationship with the Intelligence Community over the past 50 years. That healthy spirit of co-operation does not presently exist throughout the American business community, but we must find ways to build on that relationship as we move beyond the politico-military wars we have successfully waged into the economic battles that presently stalemate American competitiveness. That effort will require skilled, sensitive and committed leadership in both the public and private sectors. As difficult as the resolution of these issues will be, the situation is only going to get even more difficult if we decide that the community will play no role in the economic intelligence arena.

Editor's Note: Mr. Bass is a partner in the law firm of Venable, Baetjer, Howard & Civiletti. He previously served as First Counsel for Intelligence Policy at the Department of Justice (1977-1981)

more are appearing at the estimated rate of twelve per day. As our systems become more interconnected and interoperable, the question becomes not whether your system will become infected, but how soon and how often. Over \$100 million was spent by U. S. industry to avoid the effects of the data crime virus scheduled to wreak its destruction on Columbus Day in 1989. The Congress spent over \$100,000 to repair the effects of a single virus attack. In 1991, it is estimated that viruses caused \$1.077 billion's worth of damage. The widespread and rapid proliferation of personal computers in homes, offices and schools prevents a precise measure of the actual damage.

Malicious programs which corrupt or destroy information may not simply delete files or erase disks. In one case, the management information system used to guide a major corporation was changed by the manager of Research and Development so that the data displayed in the President's spreadsheets were altered by a few percent. The R&D manager hoped that the President, relying on his computerized analyses, would make bad decisions, be fired and the R&D manager would be chosen to replace him. As it turned out, the malicious code was detected and it was the R&D manager who lost his job.

Such attacks are especially hard to detect. One datum might be changed at random every few days. Since changes may be slight, they are not as obvious as missing files or mangled data. If alterations occur over long periods of time, even periodic backup processes may not avoid their effects. Enormous amounts of money and time may be required to recreate a corrupted data base, if it is possible to repair the damage at all.

CONSEQUENCES OF DENIAL OF AVAILABILITY

Most people don't think about, and many are unaware of, the fact that our phone system—the so called public switched network—is in reality a computer system. When we pick up our handset to make a call, it isn't obvious that modern phones are themselves computers which are connected to other computers for local calls via the local switching office, and from there via trunk circuits to other switching offices around the world. With the exception of a small number of rapidly disappearing electromechanical switches in low-density rural areas, all switching and control functions are carried out by computers. En route between switching computers, calls may traverse copper wires, coaxial cables, microwave radio links, fiber optics cables, and satellite up- and down-links. Despite this complexity, the phone system in the United States is one of the most reliable systems in the world.

Even so, at 2:25PM Monday afternoon, January 15, 1990, the AT&T long distance network comprising 114 switching centers, each containing a main and a backup computer to ensure that the system could handle every conceivable problem, began to falter. Within minutes,

more than half of all calls being attempted by AT&T customers were answered by a recorded message informing the caller that, "All circuits are busy. Please try again later." Not until 11:30PM, some nine hours later, would the network return to normal service.

The economic consequences were significant. AT&T estimates that it lost \$75 million in lost calls alone. Of 138 million long distance and 800-number calls, some 70 million were rejected by the faulty system. Many of those calls were business calls, and the failure to connect cost those businesses directly due to orders not being placed and operations being delayed or halted altogether. There were indirect costs as well due to decreased efficiency and productivity. Some businesses, like the New York Stock Exchange, had made arrangements for backup service and so were less affected; other businesses which had not had the foresight to buy backup service were out of business or severely hampered. Airlines, hotels and car rental companies lost reservations. Phoned catalog orders were not placed. Service companies could not support their customers. Undoubtedly some of the revenue those companies lost was gained by other companies that didn't use AT&T, but some were lost forever. The total economic consequences? Unknown and probably unknowable.

Unfortunately, the January, 1990 incident was not an isolated case. On June 10, 1991, more than a million Pacific Bell customers in the Los Angeles basin lost phone service for ninety minutes. Soon thereafter, on June 26 and 27 of the same year, ten million phones in four widely separated U.S. cities went down. More millions of dollars were lost.

In the world of computer systems and networks, too, there are analogies to the outages of the telephone system. The Internet is a worldwide network consisting of over 5,000 subnets, each of which connects from one to dozens of computers and terminals to any other user on the net. On November 2, 1988, a small program appeared on computers connected to the Internet. This program was a "worm"—a program (much like the computer viruses that have been widely publicized) that makes copies of itself and sends the copies along to other computers on a network. The copies make copies in turn and send them along, and the copies' copies make copies, and so on. The result is like a chain reaction in nuclear physics, and in short order the network was so busy creating and sending copies of the worm that it couldn't do anything else. In a wide-area network like the Internet upon which thousands depend, the consequences were serious.

When the Internet worm struck, it was immediately feared that the program might be a Trojan horse, an apparently innocent program that contained destructive code to be activated at some later time or date. Others were concerned that the worm was placed into the net by an enemy power, either to compromise or destroy information or to disrupt services. Many system operators were so concerned that they shut down their com-

(continued on page 30)

hosting such plants. Americans who have invested in Honda have been winners, and even American car companies are better off ultimately because they have had to become more efficient and productive to meet the foreign car challenge posed by Honda and other foreign car makers.

The list of winners and losers from even the limited example of imports of Honda automobiles goes on and on, but suffice it to say that in economics, competition is not a black and white, zero sum game. "America" does not "lose" when faced with foreign economic competition. That competition poses challenges to various sectors of the U.S. economy which must be overcome is certainly true, but we are not talking about threats to our national existence.

A fundamental change. Undertaking a program of providing direct intelligence support to the U.S. private sector would be both a significant departure from past practice and a major operational challenge. Therefore, it should be incumbent upon those who advocate such an effort to describe how it would be accomplished. Rather than making their case, however, proponents usually sidestep or ignore this critical point. Indeed, Adm. Turner blithely states, "There are problems galore, but these are for the Commerce Department to handle on a case-by-case basis." There are certainly "problems galore," but they are beyond the ability of the Commerce Department or any other government agency to resolve.

Practical concerns. The first significant problem is the matter of practicality. Attempting to define a workable program to share intelligence with the private sector immediately raises a host of practical problems, both in how to implement a program as well as the consequence of doing so. One of the first questions to address is how a program would be set up and operated. There is, for example, the issue of defining the beneficiary. What sectors of the economy and what companies would be targeted for assistance, since the IC could not help them all? Who would make those choices? Would all companies within a particular sector receive assistance, or just some? Again, who would choose and on what basis—size, profitability, or market share? The U.S. government—the same outfit that wasted billions of taxpayer's dollars trying to support the development of synfuels in the 1970s—would need to create a mechanism to decide which sectors and companies would be supported.

The fairness and wisdom of the selection process notwithstanding, intelligence support would ultimately come to be recognized as just another subsidy, and as such, would be subject to the same vagaries of politics as any other subsidy. Anyone who is confident that the government could make wise and farsighted determinations about what sectors or companies to assist should look no further than the April 6, 1993 *Washington Post*. An article entitled, "Hair That Defies Cutting" describes

the continued existence, after 39 years, of a \$180 million-a-year program to subsidize the growth of mohair wool. Strategic necessity, economic efficiency, and other such logical measures are clearly not relevant in government (political) decision-making about who or what is to receive government support and assistance. There is no reason to be confident that decisions about which companies to provide with intelligence support would be made with any more wisdom than has been shown in the mohair support program. Companies with the biggest political clout—not the greatest strategic need—would likely demand and receive the greatest support.

"Who is Us?" Before devising a support process, however, there is an even more fundamental question: exactly what is an American company? The Commerce Department defines a U.S. company as any enterprise with a majority of stockholders and assets in the United States. But the picture is more complicated than that. In the present era of multinational corporations and voluminous international trade and investment flows, the question of nationality is becoming ever more blurred. Would overseas subsidiaries of U.S. companies be assisted? What about U.S. subsidiaries of foreign companies? Should an "American" company be provided intelligence if it would use that information to win a contract to make a product in an overseas factory, if it were in competition with a "foreign" country that, should it win the contract, would make their product in a factory located in the United States? What about "American" companies working in cooperation, via joint venture, technology sharing, or other arrangements, with foreign firms? How are those interested separated in order to share intelligence with only the American entity?

These questions are not mere abstractions, but are just some of the very real issues which must be sorted out and addressed in any intelligence support program. The following concrete example is illustrative: in February of this year, six major companies announced an alliance to develop new portable communication devices. Those companies are AT&T, Motorola, Inc., Apple Inc., Sony Corp., Matsushita Industrial Electric Co., and Philips NV. The first three are U.S.-based corporations and the last three are foreign-based. How could only the U.S. companies be helped without at least indirectly helping the foreign companies? And wouldn't helping those foreign companies hurt other U.S. companies that will surely also enter the market for such devices.

These questions about what is "American" and what is "foreign" are growing more complicated and are a consequence of an increasingly economically integrated world. One person who has closely studied these issues of national corporate identity and national economic interests is Secretary of Labor Robert Reich, during his former tenure as a teacher at the Kennedy School of Government at Harvard University. Mr. Reich pub-

(continued on page 26)

lished two compelling articles in the *Harvard Business Review*, "Who Is Us?" (Jan/Feb 1990) and "Who Is Them?" (Mar/Apr 1991), which describe the complex and fragmented nature of today's global economic environment. Some finds from the former article are instructive:

But today, the competitiveness of American-owned corporations is no longer the same as American competitiveness. Indeed, American ownership of the corporation is profoundly less relevant to America's economic future than the skills, training, and knowledge commanded by American workers—workers who are increasingly employed within the United States by foreign-owned corporations (emphasis added). So who is us? The answer is, the American work force, the American people, but not particularly the American corporation.

The issue of corporate identity promise to become more, not less complicated as the world economy continues with its rapid pace of integration. Those changes will affect a host of government policies (such as corporate taxation) besides making a new initiative like economic espionage very problematic. While determining the identity and national allegiance of corporations will become more difficult. Mr. Reich offers a straightforward answer to the question, "who is us?" (and therefore who or what is worthy of government support). It is "the American work force, the American people." Under those circumstances, it would be inappropriate for the U.S. government to provide support to entities with uncertain identities if doing so would cause injury to other, clearly identifiable American interests (e.g. the American citizens who work for foreign companies).

What kinds of intelligence? Assuming one could resolve the issue of "who" to support, other vexing practical problems would remain. What kinds of information should be shared with the private sector? Should companies be given tactical data about specific projects or contracts for which they are competing, or broad, strategic estimates about economic prospects in particular countries or regions? Considerations of what kinds of intelligence data should be shared strike at the heart of one of the canons of the Intelligence Community—protection of intelligence sources and methods.

Maintaining the security of sources and methods, while preparing the intelligence for purposes for which the entire collection and analysis system was not designed, would be a daunting task. The information of greatest use, especially for specific contracts or projects, might well be among the most sensitive and highly classified. Any "scrubbing" process to remove those aspects which might reveal the source could also remove or obscure the details that made the report useful in the first place. The IC would face a continuing conundrum: if the intelligence to be shared was too vague, it would

be useless; but if it was too specific, then it would threaten the security of sensitive sources and methods.

The reality of sources and methods. The sources and methods issue may strike some non-intelligence professionals as abstract bureaucratic pettiness, but to the professional, the issue is seminal, in some cases literally a matter of life and death. As the professional intelligence officer knows well, the technical collection systems that produce much of this nation's intelligence have cost tens of billions of taxpayers dollars and tens of millions of man hours to design, build, operate, and maintain; a single unauthorized disclosure of information derived from one of those sources can diminish if not destroy its effectiveness. In the area of human intelligence collection, the stakes are even higher. If information supplied by a human agent is compromised, his safety and security is jeopardized. In many cases, the agent risks losing his life.

Besides security, intelligence professionals must also be concerned about the productivity of their sources of information. Would current and future sources of information want to provide secrets to the U.S. government if those sources thought the information was only going to advance an American company's bottom line? Clandestine collection of information would not be the only affected area. Department of State diplomatic reporting and Defense attache reporting could also suffer if a perception were to grow overseas that anything told to U.S. government was only to be used by U.S. companies. All of this should raise a serious concern for government consumers—to the degree sources of intelligence are harmed or lost, less intelligence will be available for them.

These are realities of the intelligence business, and they cannot be ignored if intelligence products are to be shared and used outside of established security controls. Once again, real world situations would raise complications for a support program. How would the security of shared intelligence be enforced and maintained? For example, what if an American corporate office was the recipient of intelligence information about a foreign contact, and then left the U.S. company to work for a foreign competitor? Would he or she be bound by whatever secrecy agreement had been signed or by their fiduciary responsibility to their new employer? In this era of corporate shake-ups and massive personnel turnover, concerns about protecting the intelligence that would be shared are very real.

Costs to the government. Just as there are practical problems of implementation, there also would be practical consequence to an economic espionage program, and many of them would affect the U.S. government. First, the U.S. Intelligence Community is not organized currently to produce and disseminate classified information to the private sector. Undertaking such an effort would, therefore, require a new commitment of personnel and resources. In a period of declining intelligence budgets,

(continued from page 26)

the resources for a private sector program would most likely be allocated at the expense of government policy makers, who are the only economic intelligence consumers at present. Therefore, policy makers need to ask themselves if the gain to U.S. companies would be worth the possible loss of their own intelligence support.

Policy vs intelligence. A second issue for government to consider are the occasions, sometimes frequent, when the intelligence available on a particular issue is uncertain. Policy makers do the best they can in such instances, but complications could easily arise if that same uncertain information were to be shared with the private sector. The private sector consumers might decide that the intelligence contradicted policy decisions, or at least cast doubt on the viability of the policy. For example, the government might be trying to encourage private U.S. investment in a country or region, but if intelligence analysis shared with the private sector indicated that the economic prospects for that area were poor, then the American companies might well choose not to invest. Government officials would end up arguing about the accuracy of intelligence reporting and estimates not just among themselves, but also with the private sector groups they are trying to influence.

Foreign policy impacts. A final concern for the government about an economic espionage program would be its serious and deleterious impacts on U.S. foreign policy. Although the U.S. is the only remaining superpower, increasingly our influence is dependent on our ability to create and maintain coalitions of different countries to support a particular policy or achieve desired objectives. The core of many of those coalitions are the group of countries that constituted the old Western alliance. Those are also the countries that we most frequently find ourselves competing against economically. To make those countries and their companies the target of economic espionage activity on behalf of the U.S. private sector would undermine the trust and confidence that has served as the historic basis for our political alliance and cripple diplomatic efforts to build the coalitions necessary to achieve important foreign policy goals. Granted, the world is changing and the old alliance structure is not as vital as it once was. But we should at least thoroughly consider the consequences before we undertake actions that could rend the existing relationships and complicate the handling of a host of issues, such as coordinating aid by the G-7 to Russia and confronting Serbian aggression in Bosnia.

Is it useful? After practicality, a second major category of problems relates to the issue of utility. The usefulness of intelligence to the private sector has been assumed, but that assumption has not really been proven or even effectively tested. Certainly the IC produces prodigious volumes of economic and financial information, but that intelligence is produced in response to the needs and requirements articulated by

government consumers, not the private sector. There is no doubt some incidental data not being collected would be of use to a business consumer. But it would take a significant retooling of the intelligence requirements on economic issues and the processing of that intelligence to insure the routine, timely delivery of relevant information.

The dog not barking. Throughout the debate on this issue, has anyone stopped to listen to what the private sector has to say. Or to ask them if they want or need such information? Interestingly, there has been mostly silence—not one single CEO or other senior official of an American corporation has gone on the record advocating or supporting such a program. In fact, what little reporting there is suggests that businesses are at best dubious about the idea. In a March 9, 1993 *Washington Post* article, "The Idea of a CIA Linkup Spooks Some Area Executives," local executives worried that "it could give an unfair advantage to big companies," and "intelligence sharing...would run the risk of 'spoiling relationships with other countries who would become suspicious of how level the information playing field is.'" The February 22, 1993 *Time* article referenced above noted "...many U.S. executives fear that suspected CIA involvement in their business could scare off customers and suppliers overseas. They're also afraid that American companies themselves may eventually fall under the spy agency's watchful eye."

Do business executive think that the Intelligence Community has anything useful to offer? Apparently not. As one senior executive from a major U.S. corporation has said, "If a company needs the CIA to tell them what's going on in their area of business, then they're already in Chapter 11 [bankruptcy]." If sharing intelligence with the private sector is such a great idea, then why is there no demand for such support from the intended recipients? Certainly the private sector is not shy about asking for government assistance in any number of other areas, such as import restraints, foreign market access, or tax breaks. If intelligence support for business had any utility at all, we would have heard from the private sector by now.

Legality. Would a program to provide intelligence support to the private sector be legal? As is the case for most legal questions, the answer is, "it depends." A significant number of hurdles can be identified that would have to be surmounted if an economic espionage program were to be legal. First, are the existing legal authorities sufficient to justify and allow collecting and disseminating intelligence to a non-government consumer? Various enabling statutes and executive orders would need to be reviewed and possibly modified to permit a private sector support effort. Second, intelligence collected under such a program would likely include trade secrets, and the Trade Secrets Act might need changing to allow such information to be disseminated without criminal liability. Third, wire fraud stat-

(continued on page 28)

ues might also need amending if it is decided that collection of intelligence through fraud or deceit (tactics used frequently in clandestine collection) for passing to the private sector violated that statute. Fourth, the Communication Act and the Foreign Intelligence Surveillance Act might require amendments to allow dissemination of certain kinds of intelligence. Fifth, there would be a substantial risk of extensive civil litigation against the U.S. government in both U.S. and foreign courts: management and shareholders of companies not selected to receive intelligence could sue; individuals injured by products resulting from the intelligence could sue; and companies or individuals whose trade secrets or intellectual property were taken without compensation could sue.

And that's not all. Legal protection now afforded intelligence sources and methods would be weakened, as would the government's ability to defeat legal discovery and Freedom of Information requests if those requests related to information that was disseminated under a support program. Additionally, treaties of trade, commerce, friendship, and navigation currently in force might be breached, and intellectual property rights treaties and agreements might be affected. Clearly such a program would be inconsistent with the long-standing U.S. policy of "national treatment" for foreign investment (that is, foreign investment should be treated the same as domestic investment—if we are not spying on domestic companies, then we should not spy on foreign companies).

These legal concerns are largely speculative since there has been no litigation involving economic espionage that would offer a record for more certain legal analysis. Traditionally, the courts have shown great deference to the requirements of national security. But it would remain to be seen whether the courts would view intelligence support to the private sector as a bona fide national security issue worthy of special legal forbearance. Threats to corporate profits are not the same as threats to the nation's existence, and the traditional balancing of secrecy (among other intelligence equities) against other legal rights might well experience a shift in the legal fulcrum to the disadvantage of intelligence interests.

The list of legal problems, while not exhaustive, is indicative of the many pitfalls inherent in any effort to assist the private sector. Given all of the obvious legal impediments (and likely many more not so obvious problems), it is amazing that anyone in this day and age would seriously advocate such an idea. In just recent months, we have seen the Congress launch a major investigation of a fantasy like the alleged "October Surprise" from the 1980 Presidential election campaign, where there was no serious evidence of a real violation of the law. Who would be so bold (or obtuse) to launch an effort which would almost certainly violate Constitutional amendments, statutes, executive orders,

international treaties, and open exposure to civil liabilities? Intelligence officers asked to manage such a program should heed this warning: today's good idea is grist for tomorrow's Congressional inquisition.

Morality. Do the ends justify the means? This philosophical question can be applied to many issues, and it should be applied to the subject of economic espionage. If economic competitiveness is really a national security priority, then national security tools could reasonably be applied to effect a desired outcome. The legitimate requirements of national security have traditionally allowed for extraordinary measures to be undertaken. For example, the U.S. conducts espionage abroad, an activity that invariably violates the laws of the countries where it occurs. Moreover, when espionage is conducted by foreign powers in the U.S., we consider it a crime. But we countenance our own espionage activities because it serves in the defense of our nation's security.

This paper has argued that economic competitiveness is not a true "national security" issue, and so is not worthy of application of extraordinary national security measures like intelligence support. Those who make the argument that competitiveness is a national security issue, however, owe it to the rest of us to explain what other steps should be taken besides providing direct intelligence support to the private sector. Given all the difficulties in structuring an economics espionage program (as has been described), are there not some ideas that would be more timely and effective? For example, why not change the law prohibiting bribery of foreign officials so as to enable U.S. companies to win overseas contracts? Or why not change the anti-trust laws to allow the combination of more powerful American companies, the better to compete with foreign companies? If we are talking about a genuine national security threat, then we should be willing to consider other such extraordinary steps. Such sentiment, however, both in Congress and among the general public, is not now in evidence.

The other guys. A great deal of attention has been paid to the actions of other countries using their intelligence services to spy on American companies for the benefit of their domestic business. The French, according to numerous press reports, have used aggressively the resources of their intelligence services to spy on and steal information from foreign businessmen. (Pierre Marion, former head of the French external intelligence service, DGSE, has even bragged in his memoirs about French efforts to spy on foreign companies during his tenure.) IBM and Texas Instruments were among the U.S. companies to be victimized. The recent book, *Friendly Spies*, by Peter Schweizer describes economic intelligence collection activities by the Israelis, Germans, Japanese, and South Koreans as well as the French. American proponents of economic espionage make frequent reference to those incidents in an attempt to justify a U.S. program to do the same thing. These examples

(continued on page 29)

are noteworthy, however, not because they are admirable but because they are reprehensible. It is also instructive to remember the old saying, "two wrongs do not make a right." There are many examples of behavior by foreign countries that we find objectionable. The appropriate course of action, however, is to convince the country through diplomatic or other pressures to change or modify their behavior, not for us to emulate them. The actions of other countries do not justify us doing the same thing.

In any event, countries inclined to conduct economic espionage on behalf of local businesses will face growing complications. The "blurring" of companies' national identities is happening not just in the United States, but in the rest of the world as well. The economic integration occurring in Europe as a result of the EC-92 initiatives, for example, makes intelligence support by European countries for domestic companies increasingly problematic. Even France may find itself confused about who the customer for its intelligence support should be. The new conservative government has talked about selling many of the state-run companies (which have received much of the intelligence support) to the private sector. As those companies inevitably become more "European" and less "French," the French government will find it more difficult to target the intelligence to support specific French interests.

"What is sauce for the goose is sauce for the gander." The remarkable fact is not that some governments have engaged in economic espionage, as noted above, but rather that there has been, relatively, so little of it reported and acknowledged. Given the number of intelligence services around the world, and the importance of economic issues, one would expect to have seen a great deal more of such activity. Although there may be no formal treaties, the traditional western allies (with the exception of the French) feel a reluctance to conduct espionage against one another. An American economic espionage program however, would drastically change that equation. If foreign governments thought we were spying on competitors and aggressively supporting U.S. companies, it would release whatever restraints that now exist and permit them to do the same. Thus, American businessmen abroad would become subject potentially to a wide range of pressures and harassments, including entrapment, robbery, blackmail, etc. Since we would be seen as engaging in similar activity, the U.S. would have no moral standing to protest the treatment of our citizens. In addition, it is quite possible that many countries would be better at economic espionage than we would (if only because our legal protections for the individual would preclude the more heavy-handed pressures), negating the value of our own program. Since there is relatively little of such activity now, do we want to be the ones that start an "intelligence war" supporting domestic businesses?

Who will spy? It is not at all clear that intelligence

professionals would want to be engaged in an economic espionage program. Former Director of Central Intelligence (DCI) Robert Gates has stated, "Some years ago, one of our clandestine service officers overseas said to me: 'You know, I'm prepared to give my life for my country, but not for a company.' That case officer was absolutely right." Intelligence officers signed up to serve their country and defend its security. Can they be convinced that (in some cases) risking their lives—or at the very least their career success—for a company is the same as for their country? It remains an open question whether our intelligence services would extend their best efforts in support of a program like this, but is it worth the gamble? There is also the risk of corruption, less by individual intelligence officers participating in a program than by the intelligence agencies participating in a program. Those institutions would likely become targets of intense business lobbying as it seen whenever the economic stakes are high, and there could be temptations to make biased decisions about allocation of resources and effort.

"Fraught with...difficulties." DCI James Woolsey raised some eyebrows and expectations during his Senate confirmation hearing when he described economic espionage as "the hottest current topic in intelligence policy." Subsequent news stories indicate he has reached some unenthusiastic conclusions about such an effort. A *New York Times* article on April 5, 1993 quotes the new DCI as stating that such a program would be fraught with legal and foreign policy difficulties." Mr. Woolsey's disproving tone is not surprising. Anyone who gets past the rhetoric and "economic competitiveness" and closely examines the nuts and bolts details of how an economic espionage program is supposed to work cannot fail to reach the same negative conclusions.

Sound management practice (and common sense) dictates that major new initiatives should be preceded by some form of cost/benefit analysis. In the case of conducting economic espionage in support of the U.S. private sector, the costs—practical, legal, and moral—as outlined in this paper are very high. There would undoubtedly be additional costs that would surface only upon implementation of such a plan. On the other hand, the benefits of such a program are at best uncertain and quite likely non-existent. There are many policies and programs the U.S. government can pursue that will improve the competitiveness of American companies; conducting economic espionage to provide direct support to U.S. businesses should not be one of them.

Editor's Note: Mr. Fort was the Deputy Assistant Secretary of State for Functional Analysis and Research, INR in the last Administration. Previously, he served as Special Assistant to the Secretary of the Treasury and earlier, as Deputy Executive Director of the PFIAB.

puters and brought all usage, including their research and communications to a stop. Some of the computers were down for most of the following week, with attendant economic consequences.

Fortunately, the Internet worm was not a Trojan horse or other type of logic weapon. It clogged up the Internet and denied the benefits of the net to many of its users, but the program was basically benign, the result of a graduate student's research that got out of hand. Even so, the economic damages resulting from the denial of service were impressive. One estimate of the damage reached \$116 million, with up to six thousand computers affected. Damage at individual sites ranged from \$200 to over \$50,000.

Up to the attack of the Internet worm, no one had seen such a widespread network infection. But in fact, the damages were small in comparison with what they might have been had two things been true: first, today there are many more computers and more of them are interconnected on networks, so damages would be wider spread and their total sum higher. The growth of computers and networks since 1988 has been exponential in scale. The damage consequent to a similar incident today would be catastrophic; the damage five years from now would be unimaginable. Second, the Internet worm was not designed to compromise or destroy information, but merely to replicate. Had it been designed to destroy data, the economic consequences of the worm attack could have reached many times the level they did.

STEALING SERVICE

Beyond the direct and indirect consequences of failures of information systems security in protecting confidentiality, integrity and availability, both fraud and theft are information systems security problems. Computer crime may already be costing the economy as much as \$50 billion annually — more than Hurricane Andrew each year — and the total is growing every year.

"Phone Phreaks" are hackers who specialize in understanding and manipulating the telephone systems. In addition to the danger that they will inadvertently or deliberately shut down all or part of the phone system, phreaks steal services, either by fooling the system into thinking that no charge is necessary or by having their charges appear on someone else's bill. Telephone industry losses to phreaks approached \$2 billion in 1992.

Credit card fraud is another form of information systems security failure. Lost or stolen credit cards together with fraudulent use of misappropriated credit card account numbers costs credit card companies over \$1 billion per year. While much of this loss might be avoided with improved information security, the credit card companies treat such losses as simply a cost of doing business. The losses are quietly passed along to their customers in the form of higher rates, and the

Country's economy is the loser.

Still another form of loss occurs when computer time is stolen by unauthorized users. In 1991, computer hackers cost the United States economy more than \$164 million. One hacker logged up a significant amount of stolen computer time on a supercomputer by breaking into the system and playing computer games. In another case, over half of the log-ons to an unprotected Government computer were unauthorized. Two-thirds of the same system's use time was by users who didn't have valid accounts and weren't supposed to be on the system. This means that the system was three times as large as was needed to perform the actual work for which it was intended. Assuming that the system was sized based on experience, millions of tax dollars could have been saved by buying a system properly sized to the work intended. There are also increased operational and maintenance costs which dwarf the original investment and more than offset the cost of the computer security that would be needed to prevent unauthorized use.

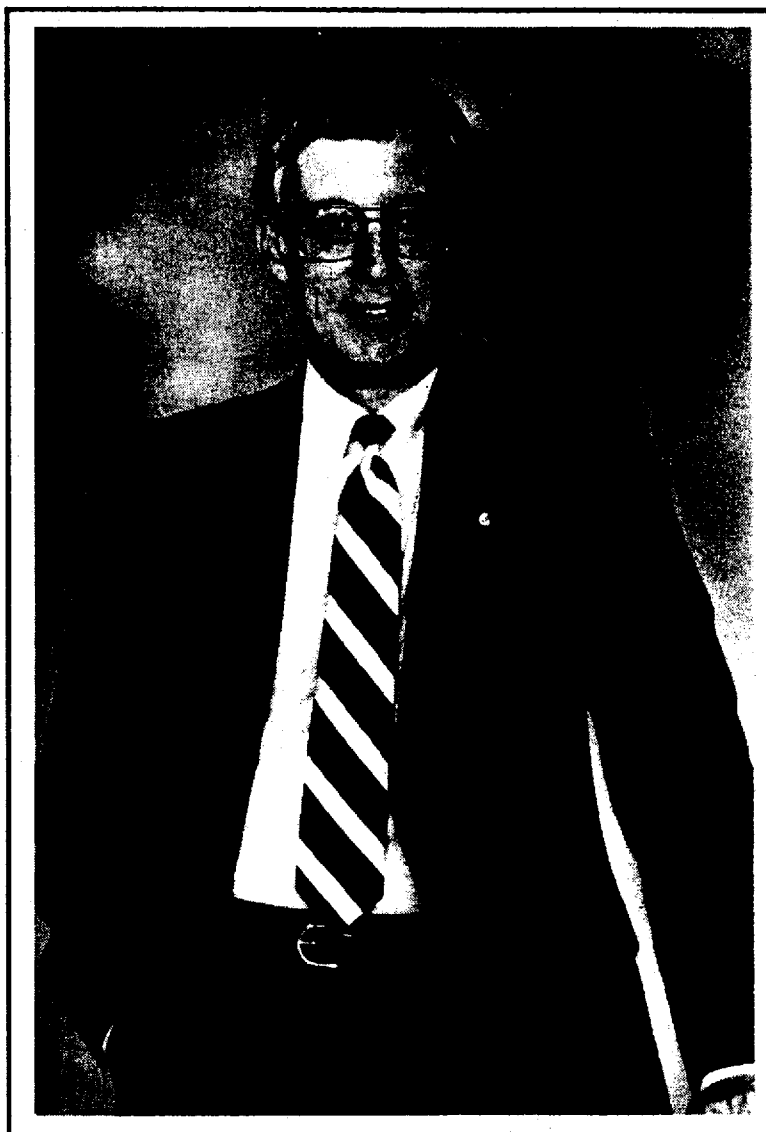
CONCLUSIONS

Information systems security costs money. The Government and private industry together spend billions of dollars for communications security, computer security, physical security of information and information processing systems, and personnel security in order to protect information assets. However, the cost to our economy of not securing our systems and protecting our information is already high and is potentially much higher. Individual instances of failure of confidentiality, integrity or availability have cost hundreds of millions, and the cumulative costs of failures are astronomical. Cumulatively, the costs of information systems security failures already equal or exceed the cost of Hurricane Andrew in most years. In the past, the diversity of our systems and networks has protected us, at a cost to productivity that we cannot sustain if we are to be competitive in world markets. But greater connectivity and greater interoperability mean greater vulnerability, both to accidents and to malicious attacks. In the worst cases, the entire economy could be damaged and the Country consequently put at risk.

The challenge is great. Fortunately, technology together with well-planned and executed security procedures can ensure the confidentiality, integrity and availability of our information assets. As part of the Global Village, we will then be able to safely share in the rich exchange of information needed to support competitive economic activity.

Editor's Note: Dan Ryan is the Director of Information Systems Security for the Office of the Secretary of Defense at the Pentagon.

1931 - CHARLES RICHARD LORD - 1993



On 3 February 1993, Charles Richard Lord, Chairman of the SASA Board of Directors, passed away at Johns Hopkins Hospital in Baltimore, Maryland.

Dick, as he was known to family and friends, entered the military in 1954, serving in the Army Security Agency and subsequently transferring to the National Security Agency in 1958 where he remained until he retired in March 1988. Throughout his entire NSA career, Dick served in operations posts at the Headquarters and overseas, acceding to the post of Deputy Director for Operations in 1982. Two years prior to his retirement he was designated the Deputy Director of the agency.

He joined E-Systems, Inc. in August 1988, and was designated Vice President for Technology Planning and Analysis. He was also "overseer" of both the company's IR&D and Advanced Technology efforts and the activities of the Center for Advanced Planning and Analysis (CAPA).

Dick was born in Omaha, Nebraska, 4 April 1931. He

held an A.B. degree from Denison University (1953) and an M.A. degree in International Relations from the University of Michigan (1954). He was also a graduate of the National War College and the Army Language School at Monterrey, California.

During his government career, he received the NSA Meritorious Civilian Service Award (1975) and the Exceptional Civilian Service Award (1980) and twice received the Distinguished Cryptologic Executive Award (1982, 1987). In 1983, Dick was awarded the Department of Defense Distinguished Civilian Service Award. He also held the National Intelligence Distinguished Service Medal and the President's Distinguished Civilian Executive Medal, both awarded in 1988.

Dick is survived by his wife, Joan, and three children, Lisa, Shelby and Todd, all living in Annapolis and a brother William B. Lord of Tucson, Arizona.

Dick Lord was a gifted professional, a family man and a good friend—he is sorely missed.

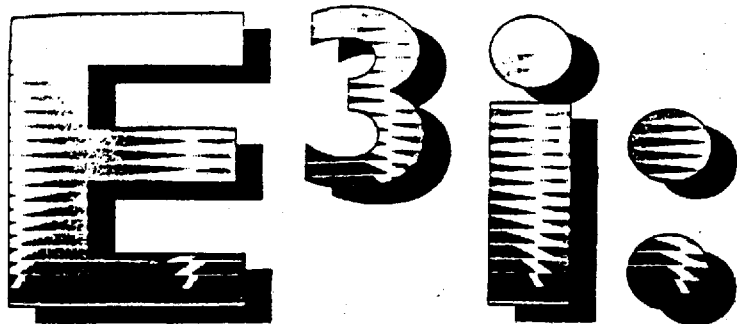
.JEM

Security Affairs Support Association
141 National Business Parkway, Suite 112
Annapolis Junction, Maryland 20701

Mr. Robert D. Steele
1914 Autumn Chase Court
Falls Church, VA 22043



Colloquy, May 1993



Ethics, Ecology, Evolution, and Intelligence

Government is not built to perceive large truths; only people can perceive great truths. Governments specialize in small and intermediate truths. They have to be instructed by their people in great truths. And the particular truth in which they need instruction today is that new means for meeting the largest problems on earth have to be created.

—Norman Cousins¹

The shock waves from the collapse of communism are still destroying historic old structures, particularly in Washington. Change agents, long dormant or ignored, are suddenly popular.

Not long after I read "Army Green" (p. 58) and met John Petersen, author of "Will the Military Miss the Market?" (p. 62), I started getting faxes from a fellow in the U.S. Marine Corps Command, Control, Communication, and Intelligence Department. Robert D. Steele wanted to talk about his hopes for restructuring the intelligence mission and redefining national security. And he wanted me to talk to representatives of the intelligence community about transforming themselves into an intelligent community. I greeted his ideas with polite skepticism, to which he responded by sending me some of the things he had written for intelligence journals about "open-source" intelligence. That means making intelligent use of publicly available information, instead of covert and classified sources. There are some wild-eyed radicals out there, all right, and some of them are in the Pentagon!

Who knows? Maybe Steele is a visionary, one of the first to see that the intelligence agencies of the Cold War era might be forced by circumstances to redefine their mission to take into account the dire state of the biosphere. Stronger things have happened lately.

Robert Steele, by his own description, is: "... a former Foreign Service officer and Marine Corps infantry officer, holds two graduate degrees and is a distinguished graduate of the Naval War College. He has spent most of his life in Latin America and Asia, and is of Hispanic heritage. As a Marine Corps civilian he was responsible for standing up the new USMC Intelligence Center in Quantico, where he developed many of his views about the relative utility to his Marine Corps consumers of unclassified versus classified information." —Howard Rheingold



THE ERA OF NATIONAL intelligence, with its unsung heroes and occasional rogue elephants in the war against communism, socialism, and other perceived evils, has come to an end. The Department of Defense and the national intelligence community are striving to restructure, desperately seeking to preserve a semblance of their once massive organizations. Both are redefining their roles and missions in order to remain competitive in the budget battles of the future.

The brain and heart of the national security "firm" have always been command and control, communications, computers, and intelligence, known by the acronym C³I. I propose an alternative paradigm for the intelligence community of the twenty-first century, one which focuses on objectives and outcomes rather than sources and methods. My approach, which integrates ethics, ecology, evolution, and

intelligence (E³I), represents a radical change in perspective on what we should be emphasizing as we adapt to our changed circumstances and prepare for future challenges. Such a paradigm could be described as the "open books" equivalent of the "open skies" concept being applied to arms control: the true value of "intelligence" to our nation lies in its informative value, a value which increases with dissemination. The emphasis within our national intelligence community should be on open sources, free exchanges between government and private-sector analysts, and unclassified production.

We have an opportunity to recast our national intelligence apparatus, and truly put it in the national service — that is, the service of the public — rather than repeat its

which we must grapple if we are to manage our national security, and the intelligence community, in a responsible fashion.

First, how do we define national security? Do we limit ourselves to "megaprotection" — strategic nuclear and conventional deterrence — while ignoring domestic crime, the loss of economic competitiveness, and the degradation of our external environment and our internal competence (a combination of character and education)? If "national security" is defined as the preservation of our national culture, of our way of life, of the conditions which permit the pursuit of happiness and prosperity, then something is seriously wrong with both our defense structure (including law enforcement), and our "national" intelligence capabilities.

If the nation is defined as the citizenry and its commonweal, rather than as the political apex of the government bureaucracy, then a radical new interpretation of the mission, sources, and methods of the national intelligence apparatus is required.

history of servitude and sublimation in the shadow of a restricted, myopic group of policy-makers whose circumstances have frequently precluded long-range planning and rational (as opposed to political) decision-making. I propose to link national intelligence with national competitiveness in a very tangible way, making intelligence the apex of the knowledge infrastructure, and the catalyst for a dramatic improvement in our ability to recognize change and opportunities for advantage. Only in this way can we quickly retrain our people, retool our plants, and revise our product lines so as to maintain a prosperous, profitable nation.

There are three questions with

Second, who is the customer for national intelligence? Is it the president, who has little time to digest or consider the distilled product of a multibillion-dollar global network of human and technical capabilities? Is it the top one hundred government officials? Is it Congress? Is it a combination of congressional staffers and executive-branch action officers? Or could "the customer" include the media, the academy, and the private sector?

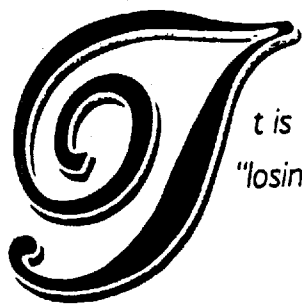
Third, given a sense of national security (however defined) and an adequate definition of the customer base that national intelligence is meant to serve, the final question must be: "What is our objective?" To what end do we wish to main-

tain a national intelligence capability? Is it to warn us of threats (unprovoked nuclear attack, biochemical terrorism, computer "hit-and-run" assaults)? Is it to inform us of systematic campaigns to undermine our economy, our sociology, or even our biology? Or is it part of a "commonwealth" sensor system, intended to monitor our internal and external stability, to educate our officials, our citizens, and our foreign partners regarding emerging conditions, organizations, and personalities inimical to "steady-state" evolution? If the nation is defined as the citizenry and its commonweal, rather than as the political apex of the government bureaucracy, then a radical new interpretation of the mission, sources, and methods of the national intelligence apparatus is required.

Such an interpretation is intended to make national intelligence more relevant to what should be two top national priorities: the preservation of our culture and a strong ethical foundation for that culture; and the preservation (indeed, the restoration) of our environment. Intelligence can play a very significant part in the recasting of our national government and its relationship with the private sector; intelligence can be teacher, mentor, lifeguard, and coach. National intelligence is an essential element of our national competence, vision, purpose, and cohesion. Only a small fraction of national intelligence should be "classified": while some classified information is essential to effective diplomacy and executive action, the classification and restriction of knowledge are inherently counterproductive and fraught with the risk of corruption.

Ethics and Intelligence

After seventeen years' experience in government, I am convinced that secrets are inherently pathological, undermining reasoned judgment and open discussion. With the exception of relatively limited technical information and



*t is now clear to all of us that we are
"losing our mind" as a nation.*

some information about plans and intentions, most of what we want to know is readily and cheaply available through the art and science of scholarship and personal interaction.

It is one of the great tragedies of our time that scholarship has lost so much ground, has been forced into mediocrity by the pressures of time, overload, and plain human failure. A lack of ethics and credibility in the academic community leads directly to ethical abuse in the intelligence community, for even when hiding behind secrets, the intelligence community has always been vulnerable to the detection of ridiculous assumptions by articulate and insightful scholars.

A wise man once said, "A nation's best defense is an educated citizenry." One could make the case that knowledge is the foundation of democracy, and that without an "open books" approach to national knowledge, we are destined to become the slaves of the rich, or worse. The purchasing and securing of patents for more fuel-efficient engines, "indestructible" polymeric paints, and other good ideas, solely to protect investments in archaic industrial plants, illustrate the problems that occur when knowledge is treated as property. Individuals end up paying much more for certain products, both because of inefficient production processes and because there is insufficient knowledge of external diseconomies such as pollution and waste.²

My proposed paradigm in no way allows for the establishment of a government monopoly on information handling, or government control over the way we manage data

and knowledge. On the contrary, this paradigm forces the issue of "who owns knowledge?" (I maintain it is in the public domain) and severely limits the degree to which any organization, in or out of government, can withhold knowledge from the public.

Environment and Intelligence

We are our own worst enemy. Although there is a healthy increase in interest by our national leadership in environmental intelligence, it is directed outward. The data obtained by national intelligence about external environmental conditions and practices must be fully integrable with state and local data on environmental conditions and practices. Only in this way can we reasonably assess the "cost" of a specific product in relation to both inefficient production processes (which consume raw materials in excess, and produce waste and pollution which also "cost" the individual in terms of resources, time, and money required for mechanical disposal), and environmental degradation. Taken in combination, what we are doing to the environment through tacit sanction by our national energy, trade, defense, housing, and education policies is far worse, every day, than a whole series of Chernobyls.³

Evolution and Intelligence

The Cold War cost us both resources and perspective. Because of the Cold War, we paid no attention to "lesser" threats and circumstances which, we are now begin-

ning to recognize, represent a cumulative threat to our survivability and prosperity. These are subtle threats, difficult to observe and understand, and the remedies are also subtle, difficult to articulate and implement. As a result, we are now in the same position as a forest ranger who, for being so intent on avoiding the bear, fails to see the encircling fires. Now both the ranger and the bear are about to be burned alive.

Evolution requires recognition of change, flexibility of posture, and fleetness of adaptation. There are only two ways to "force" evolution: through overwhelming force, a role this nation will never accept (we *could* have turned our forces loose on the Middle East and totally eliminated all weapons in both the Arab coalition and Israel); or through education. This latter approach (the preferred solution for a democracy) requires an educated citizenry. It is now clear to all of us that we are "losing our mind"⁴ as a nation; I see national intelligence, and a presidential initiative in conveying to every citizen the nature of the nonmilitary threats to our survival, as the only means of catalyzing our educational system into reform. From education comes evolution — the alternative is deepening depression and ultimate chaos, as the nine regions of North America choose to fend for themselves, and ethnic fragmentation takes its toll on the commonweal.

Where do we start? I see intelligence as part of a continuum, or a larger national construct, which must also include our formal educational process, our informal cultural values, our structured information-technology architecture, our informal social and professional networks for information exchange, our political governance system extending not only internationally but down to the state, local, and citizen level; and, as traditionally defined, as an integral element of the federal bureaucracy.

Again, with a genuflection toward

civil libertarians, I must stress that my "open books" approach to a national knowledge architecture in no way creates a government monopoly or increases government opportunities to impose "necessary illusions"; on the contrary, this approach to knowledge represents a radical departure from the current practice of allowing organizations to conceal and manipulate knowledge against the common interest.

On this basis, one can suggest that Congress and the Executive would be seriously remiss if they were not moving aggressively toward a national open-systems architecture and simple, direct connectivity between public and private educational institutions (e.g., reference librarians and library search systems); corporate marketing and research centers; state and local government information centers; ethnic, religious, and other cultural information "gatekeepers"; and, ultimately, any citizen's computer terminal.

That is the long-term objective. A measure of our situation today is the degree to which the intelligence community is integrated with all of the departments of the federal government (Agriculture, Commerce, Education, Energy, Housing and Urban Development, Interior, Justice, Education), not just the traditional national security departments (State, Defense). The answer is not good. In fact, it is very bad, for even the traditional customers must receive their "intelligence" in bulky compendiums of hard-copy,

most of it overclassified, too narrowly focused, and untimely enough to be almost useless when contrasted with the flood of "good enough" open-source material (which does not need a mass of security guards to register and control the data). The nontraditional consumers at the federal level receive little or no intelligence support, and there is no systematic integration, correlation, or comparison of the open-source information they use with the secret data of the intelligence community.

Priority to People

What steps must we take today to achieve an integrated national intelligence system by the year 2001?

The intelligence community spends too much money on extremely expensive technical collection systems, whose flood of digital information cannot be processed by existing or planned methods and personnel. Less than 10 percent of what we collect with these systems is processed, calling into question the return on investment. Our analysts are few in number, and generally inexperienced — few analysts responsible for the study of a particular country, for instance, have ever actually lived in that country, learned the language, or gotten to know the social nature and cultural character of the people about whom they are supposed to be "expert."

Our analysts are also cloistered away from their customers, the policy-makers and the action

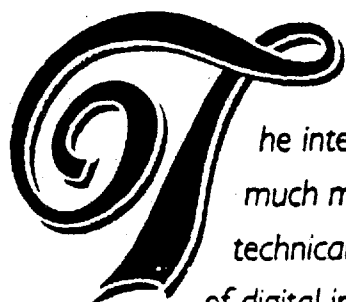
officers, and have little significant interaction with their academic, industrial, and foreign counterparts — in part because of security restrictions and in part because intelligence management refuses to give them the time to travel, train, and reflect. Analysts are instead chained to their desks, force-fed a dry diet of hard-copy intelligence, deprived of most open-source materials, and expected to "produce" sterile, uncontroversial, "objective" reports.

In my judgment, analysts should spend one-third of their time traveling and training, one-third working directly with consumers (including academic and industrial consumers), and one-third doing *analysis* that may or may not result in a product. We should nurture private-sector analysts as well as government analysts, perhaps by providing joint training programs, joint travel opportunities, and so on.

Priority to Open Sources

I have written elsewhere⁴ about our desperate need for a National Information Agency, an agency untainted and unbiased by association with the traditional intelligence community. Elements of the government now dealing with open sources should be consolidated in such an agency and granted an independent charter to enable them to support not only the intelligence community, and the remainder of the federal government that has been starved for information, but also the private sector and even foreign organizations as appropriate.

Such an agency would not be successful without a direct congressional charter and separate program, and I therefore recommend that Congress follow the precedent it created with Special Operations / Low Intensity Conflict, and create a Consolidated Open Source Program. A significant portion of the funds in this program should be used to build upon the funds appropriated for the National Security Education Act of 1991, and used



he intelligence community spends too much money on extremely expensive technical collection systems, whose flood of digital information cannot be processed by existing or planned methods and personnel.

to dramatically upgrade educational programs (beginning in elementary school) and industrial information resources devoted to our knowledge of the international physical, political, economic, and cultural environment.

Priority to Open Systems

The issues of privacy and computer security aside, there is much to be said for accelerating the electronic connectivity of the nation; as quickly as possible, every government action officer should be made accessible through Internet-like channels, and every university professor, high-school geography or history teacher, business executive, and student should be part of a national network of readily identifiable individuals with common interests.

The National Research and Education Network initiative (WER #70, p. 12) is a good one, but if we do not provide for the rural roads and comfort stations needed by *individuals*, this initiative will be of little value to the broad population of literate persons requiring rapid access to multimedia knowledge. I would move the government, including the national security structure, to an unclassified open-systems baseline, and sharply reduce the production and dissemination of classified information while increasing the availability of government-collected and -generated information to the public through electronic channels.

Consumers of intelligence — including the highest policy-making officials whom the multibillion-dollar community considers its most important customers — have often stated that they would rather have an unclassified surrogate that is "good enough to work with" than a highly classi-

fied, extremely accurate photograph or report that they cannot share with their counterparts. Analysts should be able to use classified information to inform themselves and validate their views, but they should focus production efforts on the unclassified side, providing information that can go not only to individual government consumers, but also into the public domain through open architecture.

Redefine National Security

A presidential blue-ribbon commission, comprising representatives of various industries, academic sectors, and major departments of government, should be brought together to redefine national security and our national strategic objectives. Some progress has been made in this direction through National Security Review 29; the results, which include significantly increased emphasis on the environment as a "target" for collection and analysis, are nevertheless in-

adequate, in that we have not truly come to grips with what our changed national strategy should be, nor with what changes should take place in relations between our government and the private sector, between our nation and other nations, and between US non-governmental organizations and foreign or international nongovernmental organizations.⁷

In brief, as nuclear and conventional forces cease to be the arbiters of power; as many (though not all) nation-states regress to pre-sovereign conditions; and as other forces (economics, environmental changes, and ideocultural movements) come to the fore as key areas of competition and challenge, we need to redefine who our national intelligence consumers are. In economic warfare, our private sector (industry, academia, and the citizenry) provides the "troops," and thus requires the kind of support that intelligence has previously provided to the tactical commander. In ideocultural competition, it is primarily private-sector organizations

Notes

1. *The Pathology Of Power* (Norton, 1987).

2. For an interesting examination of how an industrial system also undermines the moral foundation of a society — kinship — and thus establishes the foundation for national and industrial decision-making against the best interests of people *qua* people, see Lionel Tiger, *The Manufacture of Evil: Ethics, Evolution, and the Industrial System* (Harper & Row, 1987).

3. Walter Truett Anderson's *To Govern Evolution: Further Adventures of the Political Animal* (Harcourt, 1987), while as yet obscure, is in my judgment as important to our future as the *Communist Manifesto* was to Lenin and company. If Anderson or someone like him is ever president, I want to be his national information advocate.

4. I take this notion from Chester E. Finn, Jr.'s *We Must Take Charge: Our Schools and Our Future* (Free Press, 1991); two other books of note, both focused on content, character, and culture, are those of Allan Bloom, *The Closing of the American Mind* (Touchstone, 1987) and William J. Bennett, *The Devaluing of America: The Fight for Our Culture and Our Children* (Summit, 1992).

5. I take this phrase from Noam Chomsky's *Necessary Illusions: Thought Control in Democratic Societies* (South End, 1989). See also Edward S. Herman and Noam Chomsky, *Manufacturing Consent: The Political Economy of the Mass Media* (Pantheon, 1988).

6. "Applying the New Paradigm":

that require an improved understanding of their "competition" and of the demographic playing field upon which they are competing. We no longer need multibillion-dollar investments in systems designed to cover strategic nuclear missiles; instead, we need a multibillion-dollar investment in national knowledge architectures, and global collection, analysis, and dissemination sources and methods that are *open, free, and unclassified*.

These thoughts are consistent with those of Mitch Kapor and his concept of a National Public Network (WER #74, p. 72). My point is a simple one: national power ultimately stems from the people, even if that power might be abdicated by the people or co-opted by the rich and political. Knowledge is power, and one could say that the people require and will obtain knowledge in one of two ways: by participating in a cooperative venture in which the government facilitates and nurtures information exchange, in much the same way that it facilitated interstate com-

merce; or through revolution, in which the people, aided by hackers, break open the vaults of knowledge and refuse the government and private-sector organizations their current privileged access to knowledge that merits dissemination and exploitation.

For those concerned about the protection of privacy, with civil-libertarian issues, I would again stress that my concept of national intelligence is focused on collecting predominantly open information about conditions and entities beyond our borders, for the purpose of informing our public and private persons; my concept does not call for the collection of information about people within our borders — in fact, were knowledge about our people necessary (for demographic studies, census reviews, etc.), I would be among the first to call for "electronic aliases" in which it would be illegal to associate a true name with any compiled information about more than one person. By stressing the prominence of *unclassified* information, we essentially

provide our public with an "open-books" approach to knowledge and government management, while significantly increasing the synergy between private-sector data and public-sector data.

Our progress in taming the electronic frontier must be accompanied by a maturing of our national policies and laws; without such changes in the political and legal environments, technical progress will exacerbate the conflict between citizens and organizations, leading ultimately to revolution and electronic anarchy. Early adoption of an alternative paradigm — one that integrates ethics, ecology, and evolution, as fundamental aspects of national intelligence, and puts national intelligence in its place at one end of a continuum of information and education services to the people — could avoid the conflicts inherent in our current chaotic electronic environment, while accelerating our ability to recognize and adapt to changed circumstances.

As civilization has evolved, and the sources of power have changed from tribal mass to political force to financial leverage, each era has faced the challenge of adapting to change. We have reached a turning point, one where the ultimate source of power is finally recognized — knowledge. I conclude with an observation from Will and Ariel Durant, who, in their lifetime of studying civilizations, came to the following realization:

*The only real revolution is in the enlightenment of the mind and the improvement of character, the only real emancipation is individual, and the only real revolutionists are philosophers and saints.** ☛

How to Avoid Strategic Intelligence Failures in the Future," *American Intelligence Journal* (Autumn 1991), pp. 43-46.

7. I hold the view that government cannot abdicate its role in nurturing our culture and its educational foundation — that statecraft is indeed soulcraft; and that government expenditures are less important with respect to what they actually purchase in services, and more important in terms of their influence on the private sector: government expenditures should establish a foundation that encourages private sector outlays in positive ethical and environmental directions. Among the books that have influenced my thinking are those of George Will, *Statecraft as Soulcraft: What Government Does* (Simon & Schuster,

1983); William Lind, *Cultural Conservatism: Toward a New National Agenda* (Institute for Cultural Conservatism, 1987); Herbert Stein, *Governing the \$5 Trillion Economy* (Oxford, 1989); Albert L. Malabre, Jr., *Within Our Means: The Struggle for Economic Recovery After a Reckless Decade* (Random House, 1991); and David M. Abshire, *Preventing World War III: A Realistic Grand Strategy* (Harper & Row, 1988). The latter book, despite its title, is a superb description of how the president should take charge of long-term policy planning across all dimensions of our domestic and foreign environment.

8. Will and Ariel Durant, *The Lessons of History* (Simon & Schuster, 1968), p. 72.

**GETTING IT RIGHT, PART I:
GENERAL EVALUATION OF NATIONAL INTELLIGENCE CAPABILITIES**

Robert David Steele¹

Introduction to the Series

Our national and defense intelligence capabilities, while strong in many respects, are unbalanced. They are unbalanced in relation to

(1) the cycles of intelligence (i.e. excessive emphasis on technical collection, inadequate human and open source collection, and completely unsuitable and constrained analysis and dissemination), and also unbalanced in

(2) lacking direction and responsiveness to the full gamut of consumers of intelligence, both across all Departments of government, and at all levels of endeavor (strategic, theater, tactical, and technical).

At the same time, there is are two fundamental flaws in how we "do" intelligence:

(1) On the one hand intelligence professionals keep their consumers at arm's length--in fact, in the past, it has been the intelligence community who decided on which consumers would have the "privilege" of being supported;

(2) On the other hand, the intelligence community has completely ignored the flood of unclassified information reaching the consumer, and arrogantly assumed that the consumer would pay greater heed to its classified "nuggets". The actual result of

¹ Editor's Note: Mr. Steele, new to our pages, has over 18 years practical experience in the intelligence arena, including service as the founding Deputy Director of the USMC Intelligence Center, a new National Foreign Intelligence Program production facility created in 1987. Recently resigned from the Marine Corps, where he served on a number of national and defense intelligence leadership forums, he is now the President of OPEN SOURCE SOLUTIONS, Inc., a small corporation that serves as a non-profit educational clearinghouse and advises governments and businesses on how to improve their unclassified intelligence sources & methods. In 1992 he was named one of the "Microtimes 100: Industry leaders and unsung heros who made a difference in the computer industry in 1992 and helped create the future". He can be reached at voice: (703) 536-1775, facsimile (703) 536-1776; or by mail to Open Source Solutions, 1914 Autumn Chase Court, Falls Church, Virginia 22043.

this attitude has been an abdication of the policy advisory role, with consumers relying far more on the 90% of their information which is *unclassified and unanalyzed*.

This series will explore the problems and suggest changes. Part I is devoted to the first area of inquiry, the question of balance within the community; Part I explores the second area of concern, the relationship between the intelligence producer and the intelligence consumer.

Grading Performance by Agency and Level

Significant restructuring is underway, responding both to the lessons learned from Desert Storm and Desert Shield, as well as mandates from Congress inspired by severe fiscal constraints as well as a sense that all is not well with national intelligence support to military operations, and with aspects of defense intelligence. The next two years offer us all a unique opportunity for reflection and revitalization within the intelligence community.

In evaluating the degree to which the intelligence community as a whole may need realignments and redirection, it is helpful to think in terms of the four levels of executive action (strategic, operational, tactical, and technical), and to also distinguish between the four major areas of intelligence endeavor irrespective of discipline (direction, collection, analysis, and dissemination). If one desires to deepen the analysis, then applying this matrix to every executive department (without exception) will readily create a Rubric's Cube of green, yellow, and red performance indicators, or "best guess" grades.

In other words, the intelligence community can be "graded" for how well it does each of the major functions of intelligence, not only in relation to the level of analysis (and the consumers who need that level of analysis), but also in relation to how well it serves specific Departments of government. For instance, one can easily recognize how the U.S. Departments of the Interior, Education, Energy, and Agriculture have been poorly served. Even though this has been based on Presidential priorities which focused national intelligence exclusively on the interests of the National Security Council and the Departments of Defense and State, we can now see that a deepening of the consumer base is required, and that we are not doing well in relation to these non-traditional consumers of intelligence.

JUSTICE.....
 AGRICULTURE.....
 INTERIOR.....
 EDUCATION.....
 ENERGY.....
 COMMERCE.....
 DEFENSE.....
 STATE.....

Quick Looks	Direction	Collection	Analysis	Dissemination
Strategic Level	C (D)	B (C)	C (F)	D (F)
Operational Level	C (D)	D (F)	B (C)	B (C)
Tactical Level	D (F)	C (D)	D (F)	D (F)
Technical Level	B (C)	B (C)	C (D)	B (D)

Figure 1. Intelligence Evaluation Matrix

Above are my gross evaluations of how we are doing now, against the old threat and (in parenthesis) against the emerging Third World, non-conventional threats including non-military threats and circumstances. Naturally these grades could be argued by virtually anyone, but I feel comfortable--indeed, generous--that this is not an unrealistic evaluation given the changing definitions of national security.

Each box in Figure 1, then, has two distinct grades or evaluation marks: the top mark is the "school grade" for how we are doing against conventional (e.g. Soviet) target sets of interest to the traditional consumers of intelligence. The bottom mark, in parenthesis, is my evaluation of how we are doing and likely to do in the absence of major restructuring, against non-traditional targets (e.g. global environmental and energy targets, non-proliferation, potentially epidemic disease, demographic trends of international import) of concern to those who have not traditionally been allowed to sit at the high table of intelligence.

At the strategic level I am most concerned about analysis of unconventional threats and opportunities, and the reach of the analyst to the broader consumer base.

At the operational level, I do not believe we have an effective system for monitoring regional stability in close

coordination with the Country Teams, and with an eye for non-military problems. This is particularly the case since so many of the factors causing regional stability are non-military and often cloaked in cultural intangibles which U.S. intelligence analysts simply "do not compute".

At the tactical level I am most concerned about our lack of preparation to deal with warrior classes different from our own. There are four warrior classes with which we must deal in the future:

(1) High-Tech Brutes, similar to ourselves, relying on very expensive technical capabilities and huge logistics trains;

(2) Low-Tech Brutes, such as narcotics traffickers and terrorists, who present us with the "needle in the haystack" problem;

(3) Low-Tech Seers, such as the Islamic Fundamentals, or Asian gangs within our cities, whose "weapons" are of a cultural kind and difficult to understand and address; and

(4) High-Tech Seers, combining on the one hand the 13-year old Pakistani computer genius who can bring our entire telecommunications system crashing down, and the large covert and overt partnerships between governments and their industries intent on achieving major economic gains at the expense of other nations.

It should be obvious, but bears stating, that we have spent 40 years building command and control, communications, computer, and intelligence (C4I) systems oriented strictly toward conventional battle with the first warrior class, the high-tech brute. It also bears emphasis that these largely static capabilities (the North American Treaty Organization C4I architecture comes to mind) are relatively useless in confronting the other three warrior classes, or environmental disasters requiring close collaboration and the sharing of "intelligence" between military and non-military organizations including international relief organizations.

At the technical level we still do not offer the policy-maker responsible for acquisition decisions a basis for evaluating the true utility, sustainability costs, and return on investment for major systems, most of them geared to fighting a high-tech warrior class and completely unsuited for engaging the other three warrior classes.

It has been my experience that most intelligence products limit themselves to specific weapons systems, topics, or countries, and are couched in terms of the target, not in terms of the decision requiring support. For instance, I failed, as

the senior civilian responsible for standing up the USMC Intelligence Center, to persuade my uniformed colleagues that we should be producing annual unclassified reports for each mission area (e.g. artillery) in which we informed the General Officer responsible for that mission area about regional "averages" (gun size, prime mover weight, general range achieved in exercises rather than on the drawing board) as well as environmental constraints such as cross-country mobility and bridge loading data. With such annual reports, these General Officers would be far better equipped to consider (and often reject) proposals for "bigger better bangs" that are simply not supportable in the context of the expeditionary environment--a context almost always absent from our national intelligence and defense intelligence products.

We are also not ready to provide near-real-time technical intelligence support and ad hoc countermeasures, e.g. in a computer warfare environment. Our scientific & technical intelligence capabilities are static, based in large centers within the United States, and organized for long-term analysis of conventional weapons systems which develop linearly over long periods of time. We are completely incapable of routinely providing rapid tactical assessment of a technical threat, and quickly developing technical counter-measures.

As we evaluate our national and defense intelligence capabilities, it is essential that we keep in mind four major and quite distinct consumer groups for intelligence:

(1) Departmental planners and programmers, who require both strategic generalizations (rather than a flood of detailed reports about tiny parts of many problems), and "political-military" information heavily laden with "plans and intentions" information.

(2) Theater (regional) planners and programmers, who require regional generalizations, and very detailed mobility information. It merits comment that our Country Teams are not well integrated into a regional planning process, with the result that civilian disasters and disorder which could have been anticipated and addressed with civilian programs, often are allowed to proceed, for a lack of "action-inducing" intelligence, to the point that military action is required. Since the military did not budget for these contingency operations, every years see the military budget turned topsy-turvy as the various services are "taxed" to pay for operations that could have been avoided has the policy-intelligence system focused on costs and benefits of what General Alfred M. Gray, former Commandant of the

Marine Corps, called "peaceful preventive measures".²

(3) Tactical commanders, who not only require vanilla orders of battle ("bean counting", which U.S. intelligence analysts do very well), but also in-depth understanding of sustainability, availability, reliability, and lethality/accuracy issues (much harder to do, so we generally don't). Tactical commanders also require maps with contour lines. This may well be the single greatest "intelligence" deficiency. Of 67 countries and two island groups of interest to the Marine Corps in 1988, there were no (zero) 1:50,000 tactical maps for 22 of them; for another 37 there were dated maps (i.e. not reflecting roads and airfield or urban areas constructed in the past ten years) for capital cities and ports only, not for the maneuver areas. The remainder for which broad coverage was available (e.g. Cuba, North Korea) were ten years or more out of date, and therefore suffering from the same lack of accurate cultural feature information.³ The smartest thing I ever heard a Marine Corps intelligence officer say: "I don't care how much order of battle data you have, if I can't plot it on a map it is useless to me".⁴

(4) Finally, systems designers and project managers. We do well-enough at initial System Technical Assessment Reports (STAR), but I have three concerns with this group: first, there is no intelligence process to support higher-level decisions about whether a systems is really needed in cost-benefit or likelihood of utilization terms; and there is no process for assuring that expensive and technically complex systems are supportable by planned C4I systems. Fast-moving aircraft with limited loiter times and precision missiles, for instance, do not have the "sensor to shooter" framework (or the digital mapping data baseline) with which to be effective in most of the world. There are also severe deficiencies in our ability to introduce updated intelligence information into the systems design and

² General Alfred M. Gray, "Global Intelligence Challenges in the 1990's", American Intelligence Journal (Winter 1989-1990), pages 37-41, reprinted in U.S. Marine Corps Command & Staff College, INTELLIGENCE: Selected Readings--Book One (Marine Corps University, Marine Corps Combat Development Command, AY 1992-93).

³ USMC Intelligence Center, Overview of Planning and Programming Factors for Expeditionary Operations in the Third World (Marine Corps Combat Development Command, March 1990). In three volumes (Overview, Supporting Documentation, and Country Profiles), this study was unclassified.

⁴ Col Bruce Brunn, USMC, then Director of the USMC Intelligence Center, speaking to the Council of Defense Intelligence Producers at their 1992 meeting.

acquisition process.

Evaluation of Strategic Intelligence Capabilities

♦ Strategic Level

- Direction. No tracking system for consumer satisfaction, no automated integrated multi-discipline requirements database, non-traditional consumers not well represented
- Collection. Superb but ossified capability with limited utility against emerging threats
- Analysis. Cut and paste community, a few bright lights kept under tight control, too many young people with little idea of life overseas, limited language/cultural skills
- Dissemination. Cumbersome compendiums of limited utility to day-to-day decisions

Figure 2. Strategic Level Problems

A persistent problem at the strategic level is the over-emphasis on the "top 100" policy-makers in the traditional national security arena, and a relative lack of attention to the needs of action officers who formulate strategic plans, recommend programmatic actions, and identify opportunities for advantage. Also, because of the focus on the "inside the beltway" group, our doctrinal, architectural, and technical capabilities for secondary dissemination of multi-media intelligence has not until recently been satisfactory.

Evaluation of Operational Intelligence Capabilities

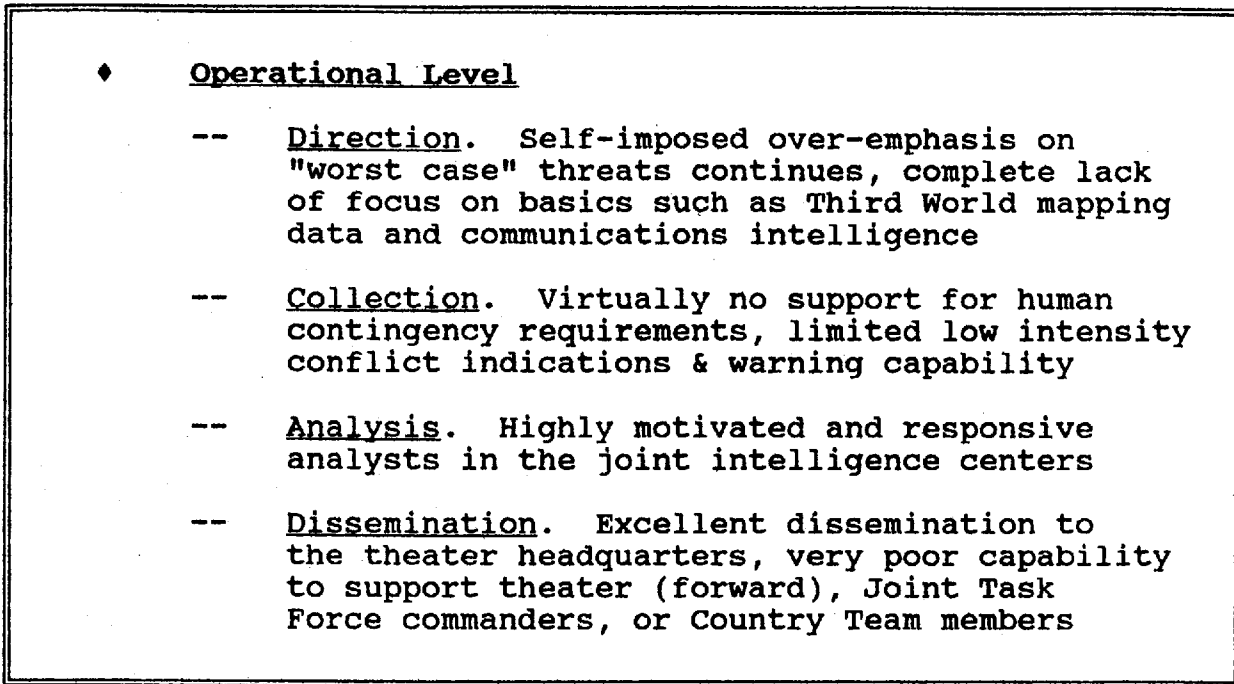


Figure 3. Operational Level Problems

Our operational capabilities have gone for so long under the premise that the Soviet Union was the main enemy, that even in theaters where virtually the entire area of operations consists of Third World countries we have paid little attention to developing encyclopedic intelligence for campaigns and contingencies in these areas.

As many of them have glaring environmental, medical, and demographic disaster problems on the horizon, this should be cause for concern for much greater remedial action than I perceive to be the case.

In addition to a lack of encyclopedic intelligence (most of which should be unclassified) there is a very limited capability to deal with these issues, in part because of a severe shortfall in analysts who are fluent in Third World languages--and of course the likelihood that our analysts might have actually lived in the country they purport to understand, is remote.

Finally, we are severely deficient in the day-to-day communications and computing connectivity and intelligence sharing conferencing and intelligence exchanges needed between

theaters, Country Teams, and parent agencies at home.⁵ We learned this the hard way in Bangladesh (Operation Sea Angel).

⁵ U.S. theaters commands have either a regional focus (such as the Atlantic and Pacific Commands) or a functional focus (such as the Transportation, Space, and Special Operations Commands). Country Teams are the Embassy principals representing the major functional agencies (State, Defense, Commerce, others) in each country where an official U.S. presence is maintained. Parent agencies, themselves fragmented into smaller fiefdoms, constitute the third part of the coordination triangle. If one adds to this C4I morass allies, regional coalition partners, international relief organizations, and host country government and private sector parties with whom C4I ties are necessary, the difficulties of non-traditional campaign planning become apparent.

Evaluation of Tactical Intelligence Capabilities

♦ Tactical Level

- Direction. From whom? How? At the mercy of national capabilities not designed to support the tactical commander, with a theater staff between the tactical units and the national organizations
- Collection. Adequate organic capabilities with exception of wide-area imagery; ground reconnaissance skills (basic patrolling) appear to have atrophied; completely inadequate prisoner handling and interrogation capabilities even when including capabilities in the reserve
- Analysis. Mixed bag, with personnel generally consumed by volumes of traffic and additional duties--they are overloaded with poor tools. Science & technology analysts fare somewhat better, but generally very poor abilities to do Intelligence Preparation of the Battlefield against unconventional opponents.
- Dissemination. Secondary imagery dissemination problems will be fixed eventually, but the lack of a realistic communications architecture to support multi-media intelligence broadcasts as well as digital mapping data suggest this will be a showstopper. Vulnerability to High Energy Radio Frequency and other computer warfare techniques will persist.

Figure 4. Tactical Level Problems

During the war in Southwest Asia the service intelligence centers, notably the Army's Intelligence & Threat Analysis Center, performed heroically. Although numerous improvements are underway, such as the transition to digital backbones, we are not yet ready for global joint inter-operable intelligence, nor are we ready for combined and humanitarian operations. As discussed in the operational intelligence section, we are simply not trained, equipped, and organized for coalition operations, and this is particularly true with respect to tactical intelligence and the communication and computing of tactical intelligence.

Evaluation of Technical Intelligence Capabilities

♦ Technical Level

- Direction. The mechanisms are well-established and the scientific & technical communities know how to get what they want--they do not always ask the right question
- Collection. Very good against the denied areas, less so against emerging technical powers and our present-day allies
- Analysis. Too much emphasis on technical countermeasures and single system threat assessments, not enough (virtually no) strategic generalizations to support cost savings in major acquisition areas by focusing on sustainability, reliability, and mobility across regions and systems
- Dissemination. Adequate, in part because the customer occupies a fixed site. As technology becomes more complex and computer warfare becomes endemic, "tactical technical" intelligence capabilities will be deficient

Figure 5. Technical Level Problems

There are two major deficiencies in technical intelligence that will require continuous policy attention in the next decade --the first is a question of sources, the second a question of methods.

-- Open sources, although better-exploited by the technical community than any other group of producers, remain a virtually untapped resource of enormous potential, while also being extremely cheap.

As selected Third World nations and present-day allies choose in the future to confront our Nation over various issues, our deficiency in this area will be recognized as a critical one. It is also a deficiency that cannot be corrected without a broad government-private sector partnership, and one which--when corrected--offers significant dividends in terms of improving private sector competitiveness without classification constraints.

-- Our methods, by contrast, while emphasizing highly

sophisticated modeling and simulation techniques, and paying very heavy attention to technical countermeasures issues, have almost completely excluded intelligence about operational geography and civil factors (road networks, hospitals, airfields) of the utmost importance in determining the general utility, reliability, mobility, and sustainability of our systems across a range of countries, not just a single country where the "worst case" threat and benign terrain are assumed. In a declining fiscal environment, when the threat itself is changing rapidly, there is no finer or more important means of responsibly reducing acquisition costs than by modifying our technical analysis methods to yield more meaningful intelligence supportive of selective procurement and surgical employment of our capabilities.

In other articles I have commented on the importance of radically altering the relationship between the analyst and the consumer (substituting the concept of distributed analysis for that of distributed production, while also emphasizing the importance of including the analyst as a member of the policy team; and I have provided an evaluation of the two bills from the Senate Select Committee on Intelligence, and the House Permanent Select Committee on Intelligence.⁶ Part II of this series, discusses the differences in perspectives between intelligence producers and consumers, and makes a case for physically moving many analysts away from their centralized and "out of touch" intelligence facilities, and into the consumer's home offices.

While I do not necessarily support legislation as the vehicle by which to resolve some of our deficiencies, and I do strongly support the restructuring efforts of both the Secretary of Defense through the Assistant Secretary responsible for these matters, and of the Director of Central Intelligence, I believe that the bills are helpful as a means of forcing us to evaluate and discourse upon certain aspects of our structure and our approach to the task of performing the national intelligence function. The above methodology, and personal comments on where I believe we stand in relation to the cycles of intelligence and the levels of endeavor, are intended to be a constructive

⁶ Editor's Note: See the companion article to this one, "Getting it Right, Part II: Intelligence Primer--How To Inform Policy". Among the author's most widely circulated other articles are "E3I: Ethics, Ecology, Evolution, and Intelligence: An Alternative Paradigm for National Intelligence", Whole Earth Review (Fall 1992); "The National Security Act of 1992", American Intelligence Journal (Winter/Spring 1992); "Applying the New Paradigm: How to Avoid Strategic Intelligence Failures in the Future", AIJ (Autumn 1991); and "Intelligence in the 1990's: Recasting National Security in a Changing World", AIJ (Summer/Fall 1990)

contribution to that discourse.

One final comment: the Vice President of the United States, and his very competent staff, have studiously avoided scrutiny of the intelligence community and integration of the intelligence community into the information policy and budget discussions underway in association with the National Information Infrastructure (NII). This is a serious mistake.

The intelligence community has never come to grips with the fundamental question about its purpose: is it in the business of producing "secrets"? Or is it in the business of informing policy? it is my view that the intelligence community is a vital part of a larger national information continuum that runs from K-12 and the universities, through private and public libraries, business and media information centers, "rest of government" information, and directly to the White House..."from school house to White House".⁷

The Vice President, as our *de facto* Chief Information Officer, has a personal interest in the training, equipping, and organizing of the intelligence community. In my judgement, there is \$1 billion a year in that budget that could be realigned toward something along the lines of a "public intelligence agency" integrated into the NII and able to provide basic (encyclopedic) intelligence about all manner of topics to our government action officers (most not cleared for secrets), our private sector enterprises, our individual citizens, and, inevitably, all citizens and organizations of the world. In this manner, the Vice President and the intelligence community could make a significant contribution to the effectiveness of our government and the competitiveness of our economy and our

⁷ This latter phrase is my adaptation from David Osborne and Ted Gaebler's Reinventing Government: How the Entrepreneurial Spirit is Transforming the Public Sector From Schoolhouse to Statehouse, City Hall to the Pentagon (Addison-Wesley, 1992). This is an important book, all the more so since David Osborne is an advisor to President Clinton and an influential participant in the Vice-President's task force to evaluate and "reinvent" the U.S. federal government. It is even more important when taken in combination with books discussing the "privatization of intelligence". Among the latter I would mention Alvin Toffler's PowerShift (Bantam Books, 1990) and his forthcoming book on information warfare and national knowledge strategies titled War and Anti-War, as well as Jon Sigurdson and Yael Tagerud (ed), The Intelligent Corporation: The Privatization of Intelligence (Taylor Graham, 1992). This last book is dedicated to Stevan Dedijer, a former member of the Office of Strategic Services, who has been very influential in developing this area of both scholastic inquiry and business practice.

citizens, while also contributing to the general prosperity of the global community.^a

^a Both Vice-President Gore, and Secretary of Commerce Ron Brown, have been invited to speak at Mr. Steele's forthcoming Second International Symposium on "National Security & National Competitiveness: Open Source Solutions". To be held at the Omni Shoreham in Washington, D.C. 2-4 November 1993, this event will be attended by 1,000 senior members of U.S. and foreign defense, intelligence, commerce, education, and environmental agencies, and their private sector counterparts.

GETTING IT RIGHT, PART II: INTELLIGENCE PRIMER--HOW TO INFORM POLICY

Robert David Steele

Conclusion to the Series

In Part I of this series, I provided an evaluation of our national and defense intelligence capabilities in relation to specific elements of the intelligence cycle, levels of analysis (and consumer), and kinds of targets. Part II concludes the series by focusing on the most fundamental deficiency in the way we "do" intelligence, and that is the disconnect between the intelligence producer and the intelligence consumer.

The Basics of Intelligence Analysis

I believe that any executive or legislative action to improve our national and defense intelligence capabilities must not only address authority and organization, but also perspective and objectives. Only in this way will we be able to accommodate both the changed nature of the "threat", the changed fiscal environment including an anticipated decline in our intelligence manpower of major proportions, and--last but certainly not least in its import--the order of magnitude changes in the external (public) information environment.

As we consider "intelligence" and its purposes, it is helpful to review some basic definitions, such as developed by Jack Davis, one of the grand masters of analysis and a recently retired member of the Central Intelligence Agency's Senior Intelligence Service. The basic information which follows regarding terminology, the differences between producers and consumers, and the barriers to analysis, owe much to Davis' course on "Intelligence Successes and Failures", and to another course he helped establish, the Harvard Executive Program's "Intelligence Policy Seminar".

Elsewhere I have provided critical commentary on the two bills proposing the "National Security Act of 1992". My view in brief is that we do not need legislation--we need instead a better way of integrating analysts and consumers, and a different approach to how we do intelligence. This article attempts to capture what I have learned from others about the barriers to intelligence success in informing policy, to include the competing influences on policy-makers and the fact that they pay no short-term price for ignoring intelligence.¹ The opinions and

¹ Despite the excellent class materials prepared by Jack Davis, and at Harvard by Richard Neustadt, Ernest May, and Gregory Trevorton, no one has ever consolidated these

the recommended remedies are my own.

INTELLIGENCE ANALYSIS

The process of producing written and oral assessments designed to improve the policymaking process by helping policy officials better understand and deal more effectively with current and prospective national security issues, including opportunities as well as threats to US interests.

ESTIMATING

The means by which intelligence professionals address aspects of national security issues that cannot be known with full confidence and thus require conditional judgements, interpretation of the evidence, and inference.

INTELLIGENCE SUCCESS

Support to the policymaking process that has the potential to assist policy officials to avoid or mitigate the damage of threats to US interests and to enhance the gain from opportunities; that is, assessments that are timely, insightful, relevant, and attention-demanding.

INTELLIGENCE FAILURE

The inadequate preparation of policymakers for an important threat to or opportunity for US interests, because of the absence of timely and attention-demanding assessments or the presentation of flawed assessments.

Figure 1. Basic Terminology

In each of the above definitions, analysis is there to inform the customer, to aid the customer in preventing or defeating threats, and in exploiting opportunities. Emphasis in each definition is my own; my point is to put "current intelligence" in perspective, to highlight the shortfalls of

perspectives into a simple public article. An earlier version of this article has been used as background reading in a course I help teach at the Marine Corps Command & Staff College, on "Intelligence and the Commander".

"research" production planned in relative isolation from the customer's decision milestones, and to drive home the fact that if the policy-maker is not reading the product and not talking to the analyst, all the authority and money in the world are not going to alter the practical outcome of restructuring.

Different Mental Maps, Different Objectives

This first look reflects the experience of generations of analysts as articulated in courses offered at the Central Intelligence Agency for their own analysts, but including participants from other organizations.

<u>Intelligence Producer</u>	<u>Intelligence Consumer</u>
♦ Believes sound policy starts with international realities	♦ Believes sound policy starts with U.S. political realities
♦ "Expert" on specific topics, immersed in their complexity	♦ Political generalist focused on solutions, simple ideas that sell
♦ Emphasizes foreign constraints, what U.S. "cannot" do	♦ Wants to focus on U.S. opportunities, art of the do-able
♦ Gravitates to most likely perceived outcome vice options	♦ Wants to understand good & bad alternatives apart from likelihood
♦ Prefers to be authoritative and avoid speculation	♦ Wants to know or at least discuss the "unknowable"
♦ "Objectivity" first!	♦ Get the job done!
♦ "We Know What You Need"	♦ "Whose Side Are You On?"

Figure 2. Producer versus Consumer, Version I

In developing our understanding of why intelligence so frequently fails to impact on policy-makers or decision-makers--even when "tailored" intelligence products are known to reach them--we must recognize the differences between the intelligence professionals (especially the analysts) and intelligence consumers (especially the policy-makers).

This difference is an important element of intelligence

failure, and so vital to understanding the need for the recommendations that conclude this article. I am therefore presenting two additional descriptions of these differences. I emphasize this aspect of the problem to make the point that changes in organization, the authority of the DCI, even significant increases in the amounts of money we invest in additional collection and information technology capabilities--these are all irrelevant if we cannot change the basic relationship between the analyst and the individual consumer in every Department and at every level.

The Academic View of Differences

At a recent running of the "Intelligence Policy Seminar" for general officers and Senior Intelligence Service officers, offered under the auspices of the Center for the Study of Intelligence and prepared by the Harvard University John F. Kennedy School of Government, Gregory Trevorton--then associated with the Council of Foreign Relations and now a senior assistant to the Director of Central Intelligence--brought out this view.

<u>Analysts</u>	<u>Policy-Makers</u>
♦ Facts/Disengaged	♦ Beliefs/Accountable
♦ Objective	♦ Intuitive
♦ "Balanced" View	♦ Agenda-Driven
♦ Long-Term View	♦ Short-Term View
♦ Descriptive	♦ Action-Oriented
♦ Employer-Driven	♦ Constituency-Driven
♦ Protect Information	♦ Use Information
♦ International Focus	♦ Domestic Focus
♦ Perfection/Accuracy	♦ "Good Enough"/Utility
♦ Written Compendiums	♦ Oral Shorthand
♦ Facts/Things	♦ People/Personalities
♦ Tenure/Continuity	♦ Short Tours
♦ Generic Audience	♦ Tight Upward Audience
♦ Single Output	♦ Multiple Inputs

Figure 3. Producer versus Consumer, Version II

As one might surmise from this organized and thorough look at the differences between our producers and our consumers, until we change the way we "train, equip, and organize" intelligence analysts (and other elements of the intelligence community) to "fit in" with our consumers and impact on our consumers, no amount of consolidated authority at the DCI level will be effective in curing our ills.

The Policy Staff View

Here I present the third and final version of these differences, this view reflecting the realities of policy staffers at senior levels of the Department of Defense, and ably articulated by Sumner Benson--a former senior analyst at the Central Intelligence Agency who successfully transitioned to a policy support role in Defense--to a number of audiences:

- ♦ The analyst is focused on all-source INTERNATIONAL DATA while the policy-maker is focused on DOMESTIC POLITICAL ISSUES as the primary criteria for decision-making;
- ♦ The analyst is focused on (and driven by community managers) to produce "PERFECT" products over a lengthier timeframe while the policy-maker requires "GOOD ENOUGH" products immediately--analysts continually run the risk of having ZERO IMPACT because their review process delays their product to the point that it is overtaken by events;
- ♦ The analyst is accustomed to INTEGRATING all-source information at the CODEWORD level, while most policy-maker staffs, and especially those actually implementing operational decisions, have at best a SECRET clearance. "A secret paragraph is better than a codeword page."
- ♦ The analyst and community management are focused on SUBSTANCE and ACCURACY while the policy maker is focused on POLITICS and PROCESS; in the latter arena, disagreement can be viewed as insubordination. Even if new information is received, POLITICAL EQUITIES may weigh against policy revision.

Figure 4. Producer versus Consumer, Version III

In short, as we evaluate the intent and utility of the two bills, we should be thinking about what we can do to increase the intellectual and the political "authority" of the analyst in terms of credibility and consumer respect. As Andy Shepard--a senior analyst manager now serving on the Community Management Staff--has noted elsewhere, such authority must rest in part on the analyst's direct access to the consumer, and a corresponding familiarity on the part of the analyst with the consumer's day-to-day as well as mid- and long-term concerns. Changing our

organization, funding, and the authority of the DCI will not significantly alter this fundamental deficiency in our national intelligence community.

Barriers to Useful Intelligence Analysis

I summarize here the barriers to analysis. These differences in perspective can also be looked at in generic terms, in the context of institutionalized barriers to intelligence success. In each case, the complexity and confusion of the environment we are trying to analyze, and the limitations of our capabilities to communicate with one another, leads to distorted and erroneous perceptions by both producers and consumers of intelligence.

<u>Signal Barriers</u>	<u>Barrier Impact</u>
♦ <u>International</u> --complexity of world affairs; multiple interests & actors; national cultural differences; impact of U.S. actions	♦ <u>International</u> --ambiguity of information; noise; paradigm bias; deception; domestic collection confusion or gaps in understanding
♦ <u>Policy</u> --misperception of foreign actors (policy mirroring); wishful thinking; policy momentum	♦ <u>Policy</u> --threat distortion; distrust of analysts; hoarding of information; manipulation of information
♦ <u>Organization</u> --resource limitations; emphasis on authoritative publications and pre-defined missions and roles; fragmentation of missions, functions, knowledge, and data	♦ <u>Organization</u> --mixed management signals if not active subversion; resistance to alternate views; information choke points (both internal and external)
♦ <u>Analysis</u> --substantive biases and cognitive traps; parochialism; monasticism; lack of exposure to real world	♦ <u>Analysis</u> --arrogance or overconfidence if not naivete; tunnel vision; resistance to outside views and priorities

Figure 5. Barriers to Intelligence Success

Such barriers are relatively well understood by students of intelligence, yet they have not been systematically addressed by either legislative charter, or executive organization. It is vital that whatever legislative or executive initiatives are taken in this watershed year of restructuring be founded on a solid understanding of this dimension of the problem. Those responsible for crafting the National Security Act of 1992, or developing a radically revised Executive Order 12333, must understand that increasing the authority of one person, the DNI, will not mitigate these predominantly cultural circumstances, and may well exacerbate the situation.

Each of these barriers has doctrinal, architectural, and technical remedies of one sort or another. In all cases the two key ingredients for improving our chances of intelligence success lie in personal relationships--the relationships between individual analysts and consumers on the one hand, and the relationships between analysts and their immediate managers on the other.

Further afield, in the collection management and individual functional areas of support (imagery, signals, human, and open source intelligence, communications and computing, training, security), equally divisive and counter-productive disparities in perspective between those "doing" and those "receiving" will further enervate the intelligence community. Specific recommendations for improvement are offered in the conclusion to this article.

Now I submit a final illustration needed to establish a foundation for remedial action.

Politicians
Executive Leadership
Legislative Leadership
Personal & Professional Staffs

<u>Government Officials</u>		<u>Foreign Officials and Organizations</u>
Department Heads	P	Diplomats
Assistant Secretaries	O	Counterparts
Program Managers	L	Correspondence
Message Traffic	I	
	C	
<u>Private and Public Sector</u>	Y	<u>Independent Researchers</u>
Lobbyists		Think Tanks
Executives	M	Academics
Citizen Groups	A	Authors
Pollsters	K	Foundations
Individuals	E	Laboratories
	R	
<u>Media</u>	<u>Personal</u>	<u>Intelligence</u>
CNN/C-SPAN	Family	<u>Community</u>
Newspapers	Intimates	CIA
Wire Services	Church	NSA/DIA
Radio/TV	Clubs	State
Pool Reporters	Alumni	Services

Figure 6. Competing Influences on the Policy-Maker

This marvelously simple yet powerful illustration has been explained to generations of analysts and managers without apparent impact on the way we do business. Note that the intelligence community is but one of many competing influences, while also lacking the political influence, economic incentives, or personal appeal such as can be brought to bear by other constituencies. There is no short-term or personal cost to the policy-maker when intelligence is ignored!

Let me drive this point home: in my experience, and in the experience of those from whom I have learned, intelligence failures are more often than not policy failures, and especially failures of character or failures of process--failures in the definition of the problem, or acceptance of the cost of good intelligence.

In the Marine Corps we teach that intelligence is an inherent function of command--yet I still do not see the

Secretary of the Navy, the Chief of Naval Operations, or the Commandant of the Marine Corps--and their three-star subordinates--coming to grips with the fact that Marine Corps intelligence is in desperate straits as a result of years of neglect by the operators--operators unwilling to assign talented people to this field, unwilling to give up a few riflemen so that tactical intelligence billets could be properly filled, unwilling to allocate training dollars to ensure good intelligence training, unwilling to integrate the intelligence professional into the operational planning cycle, unwilling to represent the Marine Corps at Navy and other flag forums where vital resource and joint doctrinal decisions are made...

It also merits comment, for those less familiar with the vagaries of public administration, that no organization is monolithic--each has its own fragmented culture to worry about, and it will not be uncommon for members of one Directorate or Bureau or Division or Service to carry entirely contradictory messages to individual policy makers, all ostensibly from the same organization. In brief then, national and defense intelligence managers are in charge of a vast conglomeration of fragmented resources, created in a piecemeal fashion over time to serve an even vaster array of consumers, most of whom do not really care one way or the other if intelligence is on their table. Only when we fail do we hear the refrain, "where was intelligence?"

Finally, and here we again confront the intelligence community's constant identity crisis over whether it is in the business of producing "secrets" or of informing policy--notice that roughly 90% of the "input" to a policy-maker's mind is both unclassified and unevaluated or unanalyzed in relation to classified sources. Certainly the policy-maker and his or her staff will attempt to integrate all of these inputs, but the people who are trained at "all-source fusion" and supposedly understand and practice analysis methods for a living are completely out of the loop on 90% of the "intelligence" to which the policy-maker actually pays attention. It is my view that we must not only expand the customer base for intelligence analysis, but that the intelligence community must be forced to undergo a radical and comprehensive "make-over" in which open sources are truly the "source of first resort" (a marvelous phrase coined by Paul Wallner, the Director of Central Intelligence's Open Source Coordinator), and intelligence analysts are comfortably fitted into the total information flow and process that feeds the policy-maker on a day to day basis.

Such is our foundation. Below are listed a few modest areas where legislative or executive arrangements may help break down some of the traditional barriers to intelligence success, and improve the ability of our dwindling numbers of analysts to render insightful, relevant, attention-demanding judgements which

prepare and encourage policy-makers for their full range of planning, programming, and execution responsibilities.

Measures to Reengineer Intelligence

Each of the four groups of ideas, as labeled, corresponds to one of the barriers of analysis outlined earlier in Figure 5.

- ♦ International Signal Barriers
 - Mandated inter-agency sharing of information at multiple-levels of security
 - Required overseas assignments for most analysts
 - Radically expanded clandestine human intelligence and overt information collection efforts
- ♦ Policy Signal Barriers
 - Annual Congressional review of "threat" in relation to each departmental activity, i.e. required "state of the world" report as precursor to Congressional review of President's budget
 - Full integration of analysts into each Department and Country Team policy process
- ♦ Organization Signal Barriers
 - Congressional and executive intelligence "Ombudsman"
 - Increased emphasis on cross-program oversight by functional area
 - Establish "return on investment" program evaluation process (not just for weapons systems, but for intelligence capabilities)
- ♦ Analysis Signal Barriers
 - Mandated inter-agency training and foreign travel for most analysts
 - Increased exploitation of foreign and domestic subject experts in development of competing "open source" analyses
 - Mandated direct consumer contact with analysts
 - Regular evaluation of analyst and product relevance and impact on decision-making to include critiques of format, medium, and timing of delivery

Figure 7. Remedial Provisions

Conclusion

Who is the customer? What do they need? How do we ensure they get what they need? These are issues which we have not considered as fully as we should in our executive restructuring efforts, and which are also not adequately addressed in the proposed legislation.

In my opinion, when you get right down to it, most individuals contemplating improvements to our national and defense intelligence capabilities appear to be thinking about block and wire diagrams and funding authority, when they should be thinking about truly changing the way we do business by substantially expanding the customer base for intelligence, redefining our national security concerns, integrating the individual analyst into the daily lives of their customers, and recapitalizing our infrastructure to take full advantage of the rapidly expanding sources of unclassified information, while also empowering our dwindling work force.

- ♦ Expand the customer base
- ♦ Redefine national security
- ♦ Integrate analysts and customers
- ♦ Recapitalize the infrastructure
- ♦ Fully integrate open sources & products

Figure 8: Prescription for Intelligence Success

If we don't come to grips with these basics, then neither the executive initiatives nor the proposed legislation will make any real difference in our national security or our national competitiveness.

There is a great deal that is "right" with U.S. intelligence, and there are many unsung heroes who have proven themselves developing "work arounds" in extremis. But the reality is that we have built up an enormous and relatively cumbersome intelligence community which has gradually isolated itself, both from its consumers, and from the "real world" of cultural complexity, fast-moving events, and changing priorities. This series has not addressed the role of the private sector as an alternative source of "national" intelligence, nor of the need to substantially improve the ability of nations, organizations, and individuals to exchange "intelligence" at will, in fluid coalitions of the moment. Therein lies the future.

What is the Secretary of Labor trying to tell us that the Director of Central Intelligence is having difficulty understanding?

**CORPORATE ROLE IN NATIONAL COMPETITIVENESS:
SMART PEOPLE + GOOD TOOLS + INFORMATION = PROFIT**

by Robert David Steele-Vivas

Vice-President Al Gore, totally loyal to President Bill Clinton and discreetly avoiding the limelight, is never-the-less the "core" performer in the Clinton Administration. Our national competitiveness--and the profits of many corporations managed and owned by U.S. citizens--depend heavily on the outcome of Al Gore's efforts to "reinvent government", and to create a National Information Infrastructure (NII). Both of these efforts depend in turn on many players, both in and out of government, but two of the players could have an especially substantive impact on how America does business as we enter the era of information warfare: the Secretary of Labor, and the Director of Central Intelligence (DCI).

Secretary of Labor Robert Reich, whose thoughts on this matter are presented in his recent book, The Work of Nations (Vintage, 1991) has it right: the only way to increase our competitiveness is to invest in our *people*, providing them with continuing education, the

best information handling tools money can buy, ready connectivity to other experts, and virtually unlimited access to *information*. Product, market sector, the nationality of the individual employee, even the activities of "Friendly Spies", are distractors.

Alvin Toffler, Peter Drucker, and others have clearly established that in the age of information warfare, information is not only the ultimate source of power, but is also, as Toffler illustrates so well in PowerShift (Bantam, 1992), a substitute for time, space, labor, and capital. Information, or better stated, information tailored to a corporation's specific requirements,

Robert David Steele-Vivas is founding President & Owner of OPEN SOURCE SOLUTIONS, Inc., an organization dedicated to increasing the quality of content in our "information commons" as a means of improving both the effectiveness of government and the efficiency of the private sector.

i.e. *intelligence*, is both the core input and the core output of the successful and hence sustainable corporation .

The Director of Central Intelligence, James Woolsey, is under pressure to find ways to increase direct support to the U.S. business community by national intelligence agencies.

He is however being led down the wrong trail by his staff, focusing on how to provide industrial espionage services overseas and on how to disseminate classified information on foreign threats to our businesses. Instead, he should be focusing on what national intelligence can do to radically increase--in full partnership with the private sector--the robustness of our "information commons".

There are those who believe that no less than one billion dollars a year should be realigned from within the intelligence community budget, in order to fund this critical element of the NII.

Avoid the Cold War Mistakes of the Intelligence Community

Mistake #1: Ignore the Rest of the World ((Little People, Other Industries, Pollution, Etcetera)

One of the reasons the U.S. Intelligence Community finds itself in such turmoil, unable to satisfy many demands for its services, is because it was formed in 1947, and added to its capabilities in increments in the 40 years since then, with just one serious target: the Soviet Union. From satellites optimized for repetitive looks at Soviet missile silos, to a clandestine service and an analysis community geared largely to chasing Soviets and writing about Soviets, the existing U.S. intelligence community is simply not trained, equipped, or organized to deal with the kaleidoscope of fleeting threats and opportunities, many in the Third World, some in Europe, which can no longer be ignored.

Many corporations are in a similar situation, structured and staffed to build a specific product, for a specific market, relying on a specific natural resource. Most of these corporations do not treat information as a corporate asset, do not have a Chief Information Officer (CIO), do not have a long-range strategic intelligence plan, and have committed themselves to "no win" situations, trying to keep short-term costs down and short-term returns up, against foreign competitors who are fleet of foot when it comes to substituting labor or capital from one country for

another's.

Where the intelligence community has failed--as has the private sector--is in laying down a global unclassified information collection, processing, and dissemination grid which can be used to produce economic intelligence that is timely, easily disseminable, and actionable.

The practical outcome of this failure is that senior U.S. government policy-makers--and their corporate counter-parts--are making decisions based on less than 2% of the available information.

A simple illustration will lend credence to this statement. Imagine Country "X" as having a typical Embassy or corporate office. That office, for bureaucratic, resource, and other reasons, is unlikely to collect more than 10% of the available information which might be of interest to a wide variety of consumers with distinct interests throughout the entire government or the corporation. Worse, of that 10%, roughly 80% is "spilled" enroute to corporate headquarters, either by being classified, by being sent to only one recipient with no capabilities for central filing, or by being put into a medium (e.g. hard-copy with many attachments) which does not lend itself to electronic broadcast.

Governments and corporations which do not optimize their field collection, and digitize their field reporting, are violating the first principal of Paul Strassmann's "Corporate Information Management" (CIM) concept: one-time data entry, corporate-wide accessibility. Where the U.S. Intelligence Community can make a contribution, in partnership with the private sector and, indeed, with the intelligence services of other countries, is by helping establish a "National Information Management" (NIM) approach to unclassified multi-media (imagery and signals as well as print) multi-lingual information.

In brief, U.S. government and the U.S. private sector should cooperate to the maximum extent possible in securing for our national "information commons" the maximum possible amount of unclassified multi-media multi-lingual information. This means avoiding redundant collection and processing, and it means much improved electronic connectivity between unclassified government databases and non-proprietary corporate databases. It probably means a totally new approach to data structure and data security by all organizations in government and in the private sector.

Mistake #2: Assume Your Chosen Consumers Are Happy

There is another mistake made by the intelligence community which may also be found in those corporations that do make an investment in "competitor intelligence". That is, to assume, without any basis, that the "pearls" of intelligence will be recognized and appreciated by the managers whom intelligence has chosen to smile upon.

The reality is that classified or competitor intelligence is less than ten percent--some would say less than one percent--of the daily information intake of a senior government or corporate executive. What does this mean? *It means that fully 90% of the information reaching a senior executive is both unclassified and unanalyzed.*

The intelligence community, preoccupied with producing "secrets", has over the years abdicated its originally envisioned role, that of "informing policy". As "open sources" (what most people call public information) have exploded in richness and accessibility, the intelligence community has been left behind, locked in its vaults, smug in a "virtual unreality" of its own making. Competitor intelligence in

the private sector, in part because of the weakness of many corporations in the strategic planning arenas, appears to reflect a similar myopia, and does not make as strong a contribution to strategic vision and corporate reengineering as it might.

Mistake #3: Assume the President's Happiness is the Only Measure of Success

Finally, in addition to assuming that its "hand-picked" consumers would pay attention to its intelligence products, the intelligence community has failed over the years to recognize new consumers or new priorities between consumers. This has in part been caused by, and validated by, a continuing emphasis on the President as the ultimate consumer of the multi-billion dollar U.S. Intelligence Community.

The President, however, does not implement policy, and more often than not the President does not even realize a policy opportunity has come and gone. It is the individual action officers in the scattered departments of government (or, in industry, the individual customer representatives and product engineers) who are on the firing line day in and day out. They have no "standing" with the U.S.

Intelligence Community, and one suspects that their "gold collar" knowledge counterparts in industry don't get much day to day support from such competitor intelligence operations as might exist.

"Intelligence", whether national or corporate, must support decision-making throughout the organization, at every level and at every location, not only at the top.

Why National Intelligence Should NOT Provide Industrial Espionage Services

Some of the brightest minds in the U.S. Intelligence Community met at Harvard on 14 December 1991, in the context of an Intelligence Policy Seminar, to discuss "National Intelligence and the American Enterprise: Exploring the Possibilities". Although a general consensus could not be established, here are four observations from one participant:

- 1) There is no such thing as an "American" enterprise, and therefore classified information cannot be conveyed to private sector enterprises with any justice or consistency;
- 2) The most important use of classified information is to

illuminate the playing field for policy-makers, keeping them appraised of the economic warfare practices of other nations and non-government groups including conglomerates;

- 3) A routine provision of intelligence information from the government to the private sector would in all likelihood lead to a reduction of private sector investment in research & development, and a consequently unhealthy dependence on the government for "leads" from other nations' efforts--nations which have historically not been as effective as ours at creative thinking (and often much better than ours at implementation and exploitation); and

- 4) The best thing we could do for "national" competitiveness, irrespective of the nationality of owners, managers, or workers in specific enterprises, is to have a national knowledge strategy, one which creates a government-private sector partnership that radically increases the availability of open source information to every citizen, entrepreneur, and indeed, every foreigner fortunate enough to have access to the American data "supermarket". Bottom line: government needs to focus on providing *information* not services.

Information Continuum: "From School House to White House"

The information continuum of the Nation, every element of which should be in the constant service of national competitiveness, runs "from school house to White House". Our national information continuum includes K-12; the universities; the libraries (public and private); businesses large and small; the media; the "rest of government", including not only the departments of the federal government long ignored by the national intelligence community, but also state and local governments, many of which have representatives in foreign countries; and of course the national security community as traditionally defined, including the Department of State, the Department of State, the National Security Council, and the President of the United States.

Secretary Reich, in The Work of Nations, dismembers existing fiscal and monetary policy myths, and with them many of the myths of corporate competitiveness. He focuses instead on the importance of transitioning from high-volume low-cost mass production, to high-value tailored production. The following quotations are instructive:

"The new barrier to entry is not volume or price; it is skill at finding the right fit between particular technologies and particular markets. Core corporations no longer focus on products as such; their business strategies increasingly center upon specialized knowledge."

"In the high-value enterprise, profits derive not from scale and volume, but from continuous discovery of new linkages between solutions and needs." (Emphasis added).

When Secretary Reich talks about the new web of enterprise, and the web of knowledge, he is really talking about *corporate and national intelligence--intelligence as art and process, rather than intelligence as I.Q.*

This is what Secretary Reich is trying to tell us that the Director of Central Intelligence is having difficulty understanding: in the age of information warfare, it is the organization with the widest web for gathering information, with the most skilled and knowledgeable employees, with the best means of communicating, and with the most efficient capacity for acting on information and taking advantage of new information, that will be competitive--and by being

competitive, raise the competitiveness of the Nation.

Nowhere is it written that *intelligence* must be classified. In fact, what we have learned from 40 years of secrecy is that the classification of information is fraught with danger, for it protects ignorance, misleads policy, and often costs far more money than anyone had every anticipated. Openness, by contrast, is profitable. The coffee houses in Silicon Valley, where competing engineers meet unencumbered by their lawyers, are living proof of the power of openness in creating win-win corporate advances in information technology, and commensurate profits.

Where we have failed as a Nation is in establishing a national knowledge strategy. Alvin Toffler addresses this in his forthcoming book, War and Anti-War, which includes a special chapter on this specific topic. Vice-President Gore's efforts with the NII are a good beginning, but they are, at least at this time, nothing more than a telecommunications architecture. What we put over those lines, how we collect it, and how we manage it (e.g. changing copyright and patent law, using security software to ensure compensation to intellectual property owners)--these

are policy matters that are not yet on the "official" NII table.

They are, however, of vital interest to U.S. corporations, and urgently require a joint government-private sector campaign plan. The plan should include our schools.

An essential premise of any NIM plan must be that all individuals in this Nation produce as well as consume information, and that many of them are capable of producing *intelligence*, not just data or information.

One can define *data* as the raw elements of information, isolated pieces of information. *Information* one can define as collated data, of generic value. *Intelligence*, in contrast to information, is tailored to the needs of the specific consumer for whom the data was collected and the information collated. *Intelligence*, in contrast to information, is immediately actionable because it has been tailored to the interests, objectives, and actual resources or capabilities of the consumer.

If the information continuum is our lever, then national competitiveness appears to turn on two fulcrum points, one internal, one external.

Internally, we appear to require a national connectivity plan and a national information exchange system which enables every person having access to that system both to consume information, and to produce and disseminate information. Corporations must be able to tap in easily to the diverse talents contained in our universities, and indeed in some of our high schools. There is a *quid pro quo* here: the universities can collect some information and process some information (e.g. graduate student translations of selected competitor nation technical publications), but our corporations must also contribute collected and processed information to the "information commons".

Externally, the U.S. Intelligence Community, and all elements of the federal government represented overseas, have an obligation to enter into the "information commons" all unclassified information which has been collected at taxpayers expense.

The failure to introduce this information into the commons, which by definition is electronic--digital--may force the issue of whether or not a substantial portion of the U.S. intelligence community should be privatized.

Again, the corporate world has a responsibility here as well. If we understand and accept the NIM concept, then foreign multi-media multi-lingual information collected and processed (e.g. translated) by U.S. corporations and citizens must also be entered into the commons. One can only speculate as to the enormous redundancy between corporations, and between the private sector and the government, with respect to what the U.S. Intelligence Community calls "encyclopedic intelligence", i.e. basic information about foreign countries, companies, personalities, systems, and conditions.

On the Matter of Openness

There have been many articles, and many speeches, equating business with warfare, competition with combat, sales personnel with "front line troops". There has also been a natural tendency in the business community to adopt the traditional military-industrial perspective on secrecy, on maintaining high barriers to entry, and so on.

Where Alvin Toffler really distinguishes himself from other pundits of the day is in focusing on knowledge as an inexhaustible resource; a resource easily shared,

re-usable many times over; a resource able to support "win-win" approaches to competition.

What is happening here is that "world is becoming mind", and the principles of cybernetics are replacing the principles of physics as the governing "rules of the game". In cybernetics, a closed system is subject to entropy. In cybernetics, success, and particularly success in adaptation and survival, comes from having a shorter faster feedback loop than your competitor, and from having as many sensors as possible. Those corporations that spend 80% of their information capital on keeping the barn door closed are going to lose to those corporations that spend 80% of their information capital on bringing as many people through the door as possible.

In the age of information warfare, "security" comes from being so good at dealing with information that you have formulated your strategy and set implementation in motion before your competitor realizes the opportunity for innovation even exists. And you must do this many times over, day after day, product after product, without ever missing a beat.

On the Empowerment of People

It has always been fashionable to give lip-service to the claim that "people are our most important asset". More often than not, this has been an out and out lie, belied by abysmal working conditions, non-existent tools, and oppressive management oversight levied on our "best & our brightest".

Robert Carkhuff, in The Exemplar (Human Resources Development Press, 1984), invented the term "gold collar" worker, or "knowledge worker", and set forth the basic principles for managing smart people in the age of information warfare.

These are not new ideas, although some of the hot properties on the lecture circuit would pretend they were. Before Carkhuff there was Harold Wilensky, with his Organizational Policy: Knowledge and Policy in Government and Industry (Basic, 1967), and before Wilensky there was Chester I. Barnard, with The Functions of the Executive (Harvard, 1938). And others. The difference between their times and ours is that now we must mind them, or lose our place in the world.

Corporate Intelligence Strategy

Of all the books available in the fields of intelligence, information, strategy, marketing, and management, the best, the one that captures how a corporate intelligence strategy can leverage good people into a protected and profitable productive capability, is Carkhuff's. His principles are simple:

- 1) Emphasize data availability to the employee (this includes, in today's terms, digitalization of hard copy and automated routing/flagging of data);
- 2) Emphasize global unrestricted data flow (i.e. provide online connectivity between employees and everyone else, in and out of the corporation);
- 3) Emphasize decentralized data exploitation (applies to both collection and production);
- 4) Emphasize data-based policy (includes automation of historical memory and insistence of fresh "reviews of the bidding" prior to each major milestone in any given program);
- 5) Emphasize increased data products and direct access by the

consumer to organized data (don't collect what you won't process, don't process what you won't disseminate, organize data to serve the end-user executive, not the intermediary librarian or analyst);

- 6) Emphasize top-level focus on optimization of employee productivity through insistence on best tools, best training, best data, and elimination of middle-management obstacles to direct communication between your "gold collars".

The Bottom Line: We Have Seen the Enemy and He is Us

What does this all mean? It is fairly straight forward, and in total contradiction to everything they ever taught us in business school.

- 1) Invest in your best employees, even if you don't like the way they dress, talk, or act. Smart people can only get smarter and more profitable, if you give them the training and tools and connectivity to information that they require.
- 2) What you make or sell is not as important as how good you make it, how fast you sell it, and how quickly you can change over to making something completely different.

3) YOU are now the national intelligence community; YOU are part of the national information continuum; and YOU are a major player in establishing our national competitiveness.

4) Education and *intelligence* are two sides of the same coin. To be competitive, a corporation must be thoroughly integrated into our educational establishments on the one hand, and fully supportive of a national intelligence effort on the other.

5) National intelligence is not going to be helpful to U.S. enterprises unless YOU focus on and accept the need for a government-private sector partnership, and YOU discuss with your Senator or Representative the need to realign funds from classified capabilities to a public intelligence agency" capability.

6) One billion a year is there for the taking. Unless you ask for it, it is not going to be made available.

INTELLIGENCE IN THE 1990'S: RECASTING NATIONAL SECURITY IN A CHANGING WORLD by Robert David Steele



Robert Steele, the senior civilian participant in the creation and management of the new USMC Intelligence Center at Quantico, has served in a variety of assignments both in and out of DoD. His views, while personal and not official, are consistent with those of his Commandant as published in our Winter issue, and are a refreshing demonstration of strategic and forward thinking among our mid-level career intelligence professionals in the civil service.

"I am constantly being asked for a bottom-line defense number. I don't know of any logical way to arrive at such a figure without analyzing the threat; without determining what changes in our strategy should be made in light of the changes in the threat; and then determining what force structure and weapons programs we need to carry out this revised strategy." -Senator Sam Nunn

This article will discuss the changing threat in terms of six challenges critical to our over-all national security posture in the 1990's. To adapt intelligence to our new threat and fiscal environments, we must make radical and comprehensive changes in how we manage and conceptualize intelligence.

Our Environment

We find ourselves in a multi-polar and multi-dimensional environment in which a critical distinction must be drawn between the conventional threat and the emerging threat.

This distinction, first presented in the Commandant's article in the Winter issue, is straight-forward: the conven-

tional threat is generally associated with a government, conventional or nuclear in nature, represented by static orders of battle, linear in the development and deployment of its capabilities, employed in accordance with well-understood rules of engagement and doctrine, relatively easy to detect in its mobilization, and supported by generally recognizable intelligence assets.

The emerging threat...cannot be assessed...by our existing capabilities.

The emerging threat, by contrast, is non-governmental, non-conventional, dynamic or random, non-linear, with no constraints or predictable doctrine, almost impossible to detect in advance, and supported by an unlimited 5th column of criminals and drug addicts.

The conventional threat lends itself very well to conventional intelligence collection capabilities which include a strong ability at stand-off technical collection, and a fairly methodical,

repetitious, and largely bureaucratized way of doing "analysis"; the emerging threats, in sharp contrast, simply cannot be spotted, assessed, fixed, and neutralized by our existing capabilities.

The "war on drugs", and our concern over arms control (not just verification of Soviet reductions but also control of nuclear and bio-chemical weapons proliferation in the Third World) are both representative of these new threats.

Narcotics, in both the intelligence and the operational worlds, must be seen as representative of a "type" threat, not as an odious and undesirable distraction from the "real" threat.

Narcotics...is a 'type' threat...not a distraction from the 'real' threat.

The multi-dimensional nature of change in our multi-polar world must also be considered as we evaluate how best to meet these threats.

DIMENSIONS OF CHANGE

Political-Legal
Socio-Economic
Ideo-Cultural
Techno-Demographic
Natural-Geographic

Intelligence must be much more than simply political reporting or military Order of Battle "bean counting". Intelligence must be able to identify emerging sources of power and emerging sources of instability in each dimension, and forecast their rate of change.

Our emphasis on the need to modify our "world view" and our definition of what merits attention from our intelligence community in no way reduces the importance of continued attention to the Soviet Union.

Three areas in particular must be acknowledged:

- First, we must continue to monitor the strategic nuclear threat.
- Second, intelligence must be capable of monitoring "plans and intentions" of the Soviets in the decades ahead. We must be prepared to identify regression and deception, e.g. perestroika and glasnost may have a mirror image as a STRATEGIC DECEPTION, as a means by which the Soviet Union can establish its technological depth and regain its competitive edge.
- Finally, the flowering of democratic and opposition movements in Eastern Europe and Soviet Republics call for much more intelligence on the ground inside the Soviet Union and Eastern European countries, and a much greater sensitivity to the socio-economic, psychological, and cultural factors which were previously overshadowed by the military threat from the Warsaw Pact.

Having established in this way the environment within which intelligence must operate in the 1990's we can now outline each of the six challenges and what it means for our intelligence structure and the allocation of resources in FY 92-97 and beyond.

SIX AREAS OF CHALLENGE

Meeting Needs of Public Programs
I&W Methods for New Threats
Theory & Methods for CI/OPSEC
InfoTech Strategy
Requirements System
Resource Realignments

Challenge Number One: Meeting the Intelligence Needs of Public Programs

Today there is insufficient emphasis on defining and meeting the intelligence needs of overt civilian agencies, law enforcement activities, and contingency military forces.

This point has major fiscal implications well beyond those of concern to defense force structure managers.

There are two major fiscal strategies that intelligence must support: first, the strategy of "spending smart", and investing in cheaper peaceful civilian nation-building capabilities as early as possible, rather than waiting for situations to deteriorate to the point that military intervention is required; and second, the strategy of fighting a truly "total war" in which we recognize that a failure on our part to be competitive in the international trade & financial markets is tantamount to losing a "real" war.

Selected public programs not necessarily associated with "national security" in fact offer an exceptional "return on investment" in terms of enhancing our strategic depth and our position overseas.

General A. M. Gray, Commandant of the Marine Corps, recently emphasized the need for "more and better Third World intelligence...(so) corresponding resource allocations can be appropriately balanced". He went on to say:

"If threat is a factor in determining national investments in security assistance and foreign aid, then a more aggressive

program of Third World intelligence analysis and forecasting is needed if we are to justify long overdue and underfunded peaceful preventive measures in this vital area of concern and potential." (emphasis in the original)

Warriors pray for peace. General MacArthur made this point with unusual eloquence, and it remains true today. The task of the warrior is made more difficult and costs the nation much more in the lost lives of its sons and daughters as well as simple economic cost if pre-revolutionary conditions are not identified and dealt with through "peaceful preventive measures". Monitoring corruption associated with our military assistance programs, identifying popular misconceptions about our Nation that should be corrected, and understanding the true and often unarticulated needs of Third World countries are extremely important tasks that intelligence can undertake in defense of our over-all national security.

Intelligence must help us make investment decisions and evaluate our programs, with special emphasis on overt & covert programs focused on "nation-building" and/or the furtherance of our national interests.

Challenge Number Two: Indications & Warnings of Revolutionary Change

Our intelligence and foreign affairs communities have demonstrated only a limited understanding of revolutionary change, no methodology for studying the preconditions, precipitants, and actualization of such change, no

We have paid insufficient attention to open sources...

framework for ensuring collection and analysis priorities respect the importance of all the dimensions within which revolutions can occur, and no indications & warnings (I&W) capability suitable to this challenge. There are several contributing factors:

Firstly, we have never been comfortable with intangibles, and even less comfortable with abstract concepts and ideo-cultural meaning. It is far easier to count beans and compare things than it is to try to understand people, especially people whose entire psycho-social fabric is alien to our own.

Secondly, our planning, programming, & budgeting system (PPBS) perpetuates this tendency: only very large, obvious, "tangible" treats have in the past been acceptable justifications for major planned investments. All other investments, for instance in the Third World, have generally been *ad hoc* responses to crises, and therefore poorly conceived, coordinated, and effected.

Thirdly, our national skills lean to the technical, and away from the human factor. We have become so enamored of our overhead technical capabilities that we have failed to balance our

We need an entirely new theory and structure of counterintelligence..

tremendous signals and imagery intelligence (SIGINT/IMINT) collection abilities with a commensurate processing ability, and capped that with a comparative abdication in the arena of human intelligence (HUMINT). **Heavy reliance on foreign intelligence & security services, and officers under official cover, does not constitute a serious clandestine HUMINT capability.** Such a capability requires years to develop, and patience, a trait for which we are not noted. Our lack of commitment to strong language programs, longer tours, and non-official cover mechanisms facilitating access to every level and dimension of foreign societies and non-governmental groups will continue to frustrate policy-makers attempting to improve our national capabilities for "low intensity conflict".

Lastly, we have paid insufficient attention to open sources (OSINT),

and the development of an infrastructure for capturing and exploiting the vast outpouring of print and voice information about the Third World as well as more developed and technologically competitive nations such as West Germany, Japan, Singapore, and Brazil.

The community has done well in developing a capability for strategic warning of attack by a major governmental nuclear and/or conventional force, largely because of the relatively static and linear manner in which these capabilities are developed, deployed, and prepared for employment.

These facilitating conditions do not hold for the emerging threat. The threat today and in the 1990's is often not clearly associated with a government, "it may not come in conventional forms," its bearers are not constrained in any way, and their actions may be dynamic or even random as the frenzy of the moment moves them to action. Their capabilities do not develop in a necessarily linear fashion because they draw their weapons from all sources, including commercial enterprises, and their motivations are not well enough understood to permit any kind of reliable forecasting.

A great deal of work needs to be done in this arena, in terms of both substantive research, and designs & methods. Among the approaches that appear to offer some merit are those of cognitive mapping, social network theory, psycholinguistics, and good old-fashioned listening by experienced diplomats, official representatives, business and academic personnel, and agents in place.

Even more fundamental is the desperately needed commitment to realign existing and future intelligence resources toward basic analysis (not necessarily production) outside the standard political and military spheres, and in the Third World.

We must take initiatives, not simply defend ourselves. **Our methods of I&W should lend themselves to identifying opportunities for advantage as well as**

opportunities for dealing legal active blows to our present and future opponents. Failure in either area will cost billions over time and will hamper our ability to understand and correct our own vulnerabilities at home.

Challenge Number Three: New Theory & Methods of Counterintelligence

Closely related to our severely deficient clandestine HUMINT capabilities and our lack of understanding of foreign entities is our virtually complete vulnerability to penetration by representatives of non-governmental groups posing a non-conventional threat to our national security.

We must, quickly and comprehensively, begin addressing the threat posed by individuals seeking our technical secrets for economic warfare; by individuals suborned by criminal organizations, terrorist groups, and religious cults; and by individuals whose motivations we may never fathom, but whose reliability can not be determined with any assurance by our present system of background investigation.

We need an entirely new theory and structure of counterintelligence (CI) capable of dealing with both the expanded access of representatives of foreign governments, and the more pervasive and subtle threat from a virtually unlimited "5th column" of criminals and narco-terrorists.

This will require an unprecedented degree of cooperation between national agencies (including economic and financial agencies), private industry (including especially high-tech firms and financial institutions), and law enforcement agencies.

It will require a totally new and comprehensive approach to the management of information about people, an approach which must integrate legal safeguards through the development of artificially intelligent "expert systems" and the partial automation of Inspector General functions.

We must also completely reevaluate what we want to protect, and what we mean by "confidential", "secret", "top secret", and "sensitive compartmented information" (SCI). The system is so fragmented and inconsistent that even the most loyal individuals have difficulty taking it seriously.

Although efforts have been made to address these issues, we simply cannot resolve the contradictions of counterintelligence without an overarching strategy that includes personnel compensation and quality of life issues as well as a comprehensive approach to the management and security administration of both electronic and hard-copy information across agency boundaries.

We must move quickly to develop an effective means of organizing and "tagging" our electronic records with essential information about their source, classification, and control parameters, and we must develop inter-agency methods of electronic sharing which maximize our exploitation of information while affording us much greater automated auditing and alert capabilities essential to identify unauthorized or inappropriate diversions of knowledge.

We must carefully redefine both intellectual and physical properties that we wish to protect, with special reference to both technology and our own national infrastructure (water, power grids, lines of communication). We should pay particular attention to "critical" nodes in our technical systems which would if sabotaged or penetrated render irreparable harm to our gross national production and general security & public welfare capabilities.

We should be less concerned about the "illegal" export of technology - advanced information technology applications and capabilities, for instance, are developing so fast they have usually left the country years before they can be added to the "dual use" list of controlled items. More to the point, information technology (to take one example) evolves so fast that whatever is stolen is

out-dated within 6-18 months, and off the market within 36 months. **We are better off concentrating on staying ahead than on keeping the other folks behind.**

We must recast our domestic as well as our international security resources to better blend the efforts of those responsible for law enforcement, physical security, background investigations, offensive counter-intelligence, and operations. Counter-intelligence cannot be treated as a separate discipline in isolation; it must permeate all aspects of national operations in the same way that "administration" crosses all boundaries.

"Operational security" (OPSEC) requires much greater emphasis, especially in the counternarcotics arena and particularly in the execution of interdiction operations. We have given the narcotics community years in which to build up billion-dollar war chests and capabilities that in some cases exceed our own. We must be much smarter about how we plan and conduct operations in this environment.

As with I&W, CI must protect the nation against the massive costs associated with treason and compromise, or with terrorism unleashed on our population and infrastructure. **Financial & economic counterintelligence should become a recognized sub-discipline.** For the latter to be successful, there must be a closer working relationship between government and the private sector, a willingness on the part of the private sector to identify and correct its areas of vulnerability, and a national recognition that international finance & trade competition is the "second front" of the 1990's (drugs & terrorism comprising the first front).

Challenge Number Four: Developing an Information Technology Strategy

We need a national information technology architecture and management infrastructure that integrates telecommunications, computing, and analysis, and enables the full exploitation and integration of data from human, signals, imagery, and open sources.

This situation is largely of our own making: Service and professional fragmentation has been allowed to continue within a resource-rich environment where inter-operability and interchangeability of information technologies (and related multi-discipline databases) were not required. The infrastructure within the Department of Defense has at least a modicum of cohesion; the same is not true for the array of law enforcement, civilian government agencies, and private enterprises, including universities, which have had little occasion in the past to require direct electronic connectivity. Now we are discovering that knowledge is indeed power, and that the shorter the loop in exploiting knowledge, the more competitive our Nation.

We must get serious about cybernetics, and exploiting knowledge in relation rather than in isolation. This requires the development of a national electronic information & records management architecture that goes far beyond the existing plethora of database management applications and isolated proprietary or domain/agency specific databases. Every traditional function of "hardcopy" records management must be automated and integrated into every organization's knowledge management architecture.

Reliable and tested multilevel security operating systems are critical to our national knowledge management strategy and must be fielded before a

OPSEC requires much greater emphasis, especially in the counternarcotics arena...

serious program of cross-Agency and federal to private data sharing & exploitation can be considered. Much greater emphasis at the policy level is required on this topic, for without this capability four of the six challenges cannot be fully addressed. It bears comment that multi-level security may finally enable us to link operators directly to analysts, and break down the "green door" that has

isolated intelligence for so long from its consumers.

In addition, it is critical that the Services, agencies, and private industry work closely together to avoid at all costs incompatible interfaces and applications that have in the past restricted the transfer of data between applications and between users. A total commitment by all information technology vendors to "open systems" is vital to national productivity and competitiveness in the 1990's.

An important element of this information technology or knowledge management strategy must be a commitment to fund a global program to capture and make available to both government and private industry those essential open source print and voice records necessary to compete in all dimensions on international life. This will satisfy the President's desire to help U.S. business while avoiding the dangers inherent in attempting to pass classified information to selected enterprises.

As outlined by General Gray in his article, this would include digitization of newspapers and journals from Third World countries (and should include technical journals from such countries as West Germany and Japan); the establishment of a central repository of government-owned open source data bases such as those developed by the Foreign Broadcast Information Service (FBIS); A national program to digitize hard-copy records pertinent to our national interests in the Third World; and expansion of the Defense Gateway Information System (DGIS) to include management of the latter initiatives.

U.S. business overseas can make a significant contribution by assuming responsibility for digitizing open sources in specific countries or technical areas. The data entry problem is so large, only private assumption of this responsibility will permit the national strategy to succeed.

The downward trend of our demography makes an investment in

knowledge management tools imperative; the primary way we will be able to improve our national productivity in the 1990's is with a major national investment strategy focusing on advanced information technologies and automated knowledge exploitation.

Challenge Number Five: Establishing A Responsive Requirements System

We need a national intelligence requirements system that is useful in the management of resources; is cross-disciplinary, automated, & "zero-sum"; and is responsive to individual customers, allowing them to track the satisfaction of their requirements by discipline, topic, country, or timeframe.

There are a number of contributing factors, some of which are being addressed, some of which will take years to work out.

The greatest problem lies in the complete fragmentation of intelligence management over-all; between disciplines, between major management areas, and between levels and types of organizations, each committed to doing business "it's way".

FRAGMENTATION OF INTELLIGENCE MANAGEMENT	
<u>Disciplines</u>	
IMINT	
SIGNINT	
HUMINT	
OSINT	
<u>Decision Areas</u>	
Design & Methods	
Funding	
Collection Mgmt	
Production Mgmt	
<u>Levels of Effort</u>	
National	
Theater	
Departmental	
Country Team	

We have absolutely no way of evaluating our "return on investment" by intelligence discipline or by element of the intelligence cycle.

The continued fragmentation of the intelligence community into disciplines with their own "pipelines" for tasking of subordinate units and reporting of information back to their headquarters will make serious all-source fusion a virtual impossibility unless, as General Gray points out in his own article:

"Capabilities must be integrated both vertically and horizontally - inter-agency policies and practices must be developed which permit the fusion of

We have absolutely no way of evaluating our 'return on investment' by intelligence discipline or by element of the intelligence cycle.

information at every hierarchical level, beginning with the Country Team. At the same time, we should avoid redundant processing of the same information by every agency and service."

It is vital that the existing requirements system, which includes means of specifying topics of immediate interest to policy-makers as well as priorities for topics of mid-range and longer-term interest, be automated and structured so that all capabilities at all levels are working in consonance with one another. While some disciplines are undeniably more effective than others at obtaining particular types of information, they should be managed in unison and at the lowest possible level.

The second greatest difficulty is the absence of a clear consensus within the community over the purposes of our various requirements documents and processes. Although a document exists to forecast future intelligence requirements and is intended to guide investments in new designs & methods, in fact

it is both moribund and nothing more - at this point - than a rehash of the imagery requirements document from which it was born.

There is no over-all management of funding trade-offs between disciplines or between elements of the collection cycle. We still spend too much on technical collection and not enough on clandestine HUMINT or the processing of imagery, signals, and human intelligence. We spend virtually nothing on the single most valuable (and cheapest) source of intelligence, foreign public print and voice media.

Collection and production management continue to be dominated by the owners of the respective disciplinary collection resources, or the owners of the analysts. This is a major reason why we have redundant or unprocessable collection, and redundant production. The community has made great strides in eliminating redundant production, but it will not meet with full success until there is a cross-agency, cross-service mechanism for balancing collection versus production, and for balancing the needs of the Theater Commander-in-Chief and each Country Team with the needs of national policy-makers and other consumers.

There is another subtle miscue built into the system: there is no provision for weighting first-time collection and production requirements over those requirements that may have a higher over-all priority, but against which voluminous efforts have been made in the past. As we seek to address ever-changing issues and make our intelligence structure more responsive to our needs for new data, this feature must be established.

Lastly, we come to the problem of distinguishing between timeframes for the management of intelligence resources (i.e. on-year, five-year, twenty-year). This is important in each of the decision areas: design & methods, funding, collection management, and production management. Although the national

policy-makers can certainly impose "emphasis" on the individual disciplines, and get what they want if it is collectable with existing resources, they cannot expect to receive the kind of information, including "plans & intentions" and tactical readiness information, for which years are required to develop agents in place, or sophisticated technical collection systems, or sophisticated artificial intelligence applications and related knowledge bases.

We simply cannot have topics of current interest driving what should be the five-year priorities plan, and no serious twenty-year plan. What should be happening is that current requirements should drive collection and production by existing resources; the five year plan should drive the reassignment of existing resources and the development of mid-term new capabilities; and the twenty year plan should be driving the development of completely new designs and methods unconstrained by existing technical collection preconceptions, and without regard to existing "standard operating procedures".

Challenge Number Six: Realigning Resources in an Era of Radical Change

There is limited experience in managing resources in a declining fiscal environment while simultaneously identifying emerging threats and rapidly real-locating resources to meet those threats. Perhaps of greater concern, we appear reluctant to establish a flexible process for fulfilling this fundamental requirement. The bitter resistance of both the

Congress has shown a strong inclination to direct innovative solutions...

mainstream military and the intelligence community to such concepts as "low intensity conflict", "special operations", the exploitation of "open sources", and support to law enforcement agencies, all portend an era of bureaucratic helplessness

and inertia precisely at a time when innovative, flexible, cooperative efforts are going to be critical to our success and our Nation's security.

On the positive side, Congress has shown a strong inclination to direct innovative solutions where it must and where it has not been able to get constructive proposals from the beneficiaries themselves. The negative side of this is that appropriated funds are meaningless if not properly and rapidly obligated, and the budget executed. With the best of intentions, and no resort to such historic

We urgently need a streamlined budget execution process...

gambits as impoundment, the lead agencies can fail to expend funds for lack of strategic planning & programming talent, and for lack of responsive and flexible procurement & accounting capabilities. The 1990's will be characterized by extremely short resource management cycles in which some initiatives will move from conception to obligation to expenditure in under a year. The "war on drugs" is an ideal opportunity to develop, test, and refine a new process for allocating resources and restructuring capabilities under revolutionary conditions.

In order for the shortened PPBS cycle to be effective, top-level managers must be willing to delegate authority down to the project and program management levels. The execution requirements for the realignment of manning, training, procurement, facilities, and operations & maintenance are simply too complex and time consuming to permit top-down micro-management.

We must introduce the same "mission type order" style to our PPBS process as we expect on the battlefield. We must eliminate as much of the paperwork and documentation as possible, and drastically reduce requirements for top-level approval of lower-level adjustments in organization, equipment, tasks,

and production where these are consistent with strategic guidance.

In the computer field, the "rapid prototyping" approach has much to offer all of us as an example, in sharp contrast to the system acquisition and life cycle planning approach which is so detailed and lengthy that the system is obsolete before it gets to the production line.

We urgently need a streamlined budget execution process in which the individual responsible for the mission has full obligational authority over funds earmarked for that mission; e.g. the Director of a new Intelligence Center or Joint Task Force should

'Intelligence' cannot limit itself to stereotypical perceptions of what is and is not a threat...

be able to establish a grade & skill mix, hire people, buy equipment, contract for external assistance, and make structural changes to assigned facilities without being bound by inappropriate regulations and entrenched preferences of the parent organization's civilian personnel, automated data processing, and other established staff elements whose processes have grown too complex and time-consuming while contributing little of substance. One must stress that this in no way exempts the obligating official from oversight and accountability.

Put another way: if Congress authorizes and appropriates ceiling spaces and funds for a particular activity, the activity director should not then have to fight on a "second front" with his or her own bureaucracy, slugging out each personnel and procurement action throughout the budget execution - nor should the activity director have to fight on yet a "third front" against Departmental and Service financial administrators bent on "taxing", redirecting, and restricting earmarked funds.

Conclusion

The six challenges facing national intelligence in the 1990's are all linked together - success in one will serve as a catalyst for success in another, failure in any will stymie success in all. All have a direct bearing on the fiscal health of the nation as well as the soundness of its national security structure in the 1990's and the 21st Century.

We must recognize that "warfare" has once again gone through a major redefinition - we must now compete with other nations in the context of a "total peace" in which the tools for peaceful competition are every bit as important to national security as the tools of war. If intelligence does not meet the needs of our "front line", the civilian agencies implementing peaceful preventive measures and enforcing the law, then our defenses will continue to erode, and no amount of investment in "strategic deterrence" and conventional military forces will suffice.

We must place a great deal more emphasis on understanding all of the dimensions of power and change, and especially conditions in the increasingly lethal and volatile Third World. Without an entirely new methodology which affords us indications & warnings of revolutionary change in every dimension, we will be vulnerable, in the "worst case", to bio-chemical and technical terrorism as well as less threatening but ultimately more costly losses of initiative in various non-military arenas of competition.

"Intelligence" cannot limit itself to stereotypical perceptions of what is and is not a threat. Intelligence must inform decision-makers about every aspect of human endeavor upon which good order and the prospects for a prosperous future depend. Intelligence must identify emerging sources of power and opportunities for advantage as well as threats.

The other side of this coin is counterintelligence and operational security. An entirely new theory and entirely new methods of counterintelli-

gence are required. We must reassess what it is we want to protect, and we must reassess the threat at all levels, to include special emphasis on both domestic and foreign non-governmental actors. We must institute comprehensive new means of coordinating and controlling our law enforcement, intelligence, and counterintelligence resources, to include oversight mechanisms and the firm protection of the rights of our citizens. If we do not design and implement this new and comprehensive program, then we will leave at risk our most precious strategic assets: our population, our infrastructure, and our scientific & technical leads.

None of the above three challenges can be met without developing an information technology strategy which is national in scope, comprehensive (integrating telecommunications, computing, and production across government and private industry as well as academic lines), and visionary. We simply cannot afford to perpetuate the continued fragmentation of systems development and continued investments in labor-intensive computing systems which do not optimize the integration of available applications and capabilities. We must aggressively pursue means of exploiting all available sources of data, both classified and unclassified.

The establishment of a responsive requirements system within our government, one which acknowledges the importance of open sources and also focuses resources on gaps rather than

We cannot be content with simply 'cutting back' across the board. Realignments must occur, and occur quickly.

repetitive collection against the same static interests, is critical to the development of informed national acquisition strategies and the articulation of national interests. If we cannot "shorten our loop" in the acquisition and exploitation of knowledge, we simply will not be able to

identify multiple challenges and opportunities within our multi-polar and multi-dimensional world in time to be effective.

Lastly, if we are to meet the first five of these challenges, we must develop a process for realigning resources in this era of radical change. We cannot be content with simply "cutting back" across the board. Recognizing new needs, developing new initiatives, and funding research & development in all dimensions will be critical to our strategic longevity.

Realignments must occur, and occur quickly. We in the national intelligence community should plan on giving up any increase over base, and taking

from base a full forty per cent - twenty per cent to new initiatives tailored to the emerging threat, and twenty per cent to BASIC research & development in critical areas such as artificial intelligence, cognitive mapping, and the general theory of cybernetics. We must also protect the mission/program manager responding to strategic direction from Congress and the President, and buffer them from intermediate authorities seeking to undermine if not destroy new initiatives.

The complexity and lethality of the emerging threat, and the severely constrained fiscal environment within which we must plan for national security, require vision, energy, a commitment to cross-agency and service cooperation, and an understanding of Third World

perspectives, such as we have never been willing to muster.

Top down strategic guidance will probably not be forthcoming before FY 92, if then; in the interim, "bottom up" common sense, and individual efforts to move in these directions when we can, may be our best means of continuing to earn the "trust and confidence" of our President and our public.

We in the intelligence community, like it or not, must play a leadership role if then national security community is to responsibly decide how to train, equip, and organize its forces and capabilities for the 1990's.

APPLYING THE "NEW PARADIGM": HOW TO AVOID STRATEGIC INTELLIGENCE FAILURES IN THE FUTURE

by Robert D. Steele



Mr. Steele is a senior civilian employee of the Marine Corps with experience as an infantry officer and Foreign Service officer. He holds two graduate degrees and is a distinguished graduate of the Naval War College. The views expressed in this article are his own and do not necessarily reflect the official policy or position of the Marine Corps or the Department of Defense.

Reprinted with permission of
American Intelligence Journal,
a publication of the National
Military Intelligence Association.

This article focuses on three concerns of mine which are central to ensuring that the restructuring effort is meaningful. First, what "sins" of strategic intelligence persist in the face of restructuring? Second, how must the nature of the individual intelligence analyst, their working conditions, and their relationship to policy-makers change if we are to avoid strategic intelligence failures in the future? And third, how must we relate defense intelligence restructuring to a broader national effort to establish a truly national knowledge management and information technology strategy, a strategy to empower our enterprises and schools while enabling our government to make informed policy decisions in all areas?

Here are the major sins we are committing today:

(1) Excessive collection of technical intelligence (including much too much emphasis on repetitive collection against higher priorities instead of baseline collection against lower, e.g. Third World, priorities);

(2) Cursory attention to both open source collection, and the need for a

modest and redirected expansion of our clandestine human intelligence collection capability;

(3) Severe shortcomings in control over intelligence resources - those responsible for billions of dollars in each year's budget have no capability to evaluate relative returns on investment across programs or elements of the intelligence cycle, and no adequate mechanisms for ensuring government-owned capabilities are shared and not duplicated.

*...there are shortcomings
in evaluating relative re-
turns on investment across
programs or elements on
the intelligence cycle...*

(4) Mindset inertia. We still have very senior bureaucrats and appointees insisting that we maintain our traditional priorities against the Soviet

Union and major economic powers. To be clear on this problem:

(a) It will continue to be difficult for our policy-makers and senior intelligence managers to focus on the need for changed priorities because our intelligence and foreign affairs communities are at least two generations away from fully understanding the Third World and dimensions of change outside the political-military and transnational economic environment. We do not have an adequate methodology for studying the preconditions and precipitants of revolutionary change (including ideocultural, technodemographic, and natural-geographic change), and no indications and warning (I&W) capability suited to this challenge.

(b) Our entire intelligence structure, our designs and methods, do not lend themselves to being restructured and reconstituted. It is as if, after decades of learning how to build Cadillacs, our very fine Cadillac, accustomed to traveling the same super-highway back and forth, must suddenly be taken apart and put back together as an off-road vehicle able to deal with the treacherous terrain and back roads of the Third World. It is

obvious we not only need to pay much more attention to different "designs and methods", but that the fastest way to create our off-road vehicle, given our lack of resources, is by melting down and recasting some portions of the community in their entirety.

(5) Lack of accountability among acquisition managers and the intelligence professionals who support them. We spend billions on complex weapons systems which cannot be supported by existing or planned communications, computer or intelligence capabilities. This sin also merits elaboration:

(a) Many of our acquisition managers and action officers want nothing to do with classified information - their offices are not cleared to hold what they would want to hold; they tend to assume that once the Required Operation Capability (ROC) is approved that the "threat" ticket has been punched; they don't understand the intelligence community or how to make it work; no one has sponsored many of them for appropriate clearances; and they have no process for prioritizing their needs for ongoing threat support to their respective life cycles.

(b) Our concept for providing intelligence support to acquisition is flawed. We tend to focus on the technical lethality aspect of the threat, while ignoring the equally if not more important aspects of tactical reliability, operational availability (and mobility), and strategic sustainability. It makes sense to have capabilities able to deal with worst-case scenarios - it does not make sense to burden expeditionary forces with mainstream conventional weapons systems if cheaper, more mobile, and more easily sustainable alternatives are available.

(6) Finally, our worst sin, a lack of commitment to people. Our grade structure, working condition, and turnover rates (both job reassignments and resignations) leave us with a largely "un-expert" analysis population whose historical memory is both conventional (what is in the files) and of short duration. We are

not growing the kind of analyst so immersed in their topic that they can sense change and underlying analytical trends and anomalies. When someone says "protect the people in the budget", what they mean is "keep as many serfs on board as possible". They do not mean "nurture our best, give them time and money for travel, training, and reflection, protect them from day-to-day 'must have update' calls". Our personnel strategies, some of which seek to keep personnel costs down by having a "bulge" in the most junior analytical ranks, do not provide the career opportunities needed to keep the "best and the brightest" focused on analysis for an entire career, and literally drive people away from analysis and toward "management" or administrative positions, if not out the door entirely. We compound this sin by failing to provide the analysts we do have with the tools they need to manage raw multimedia data and carry out higher-level analysis tasks including pattern analysis and modeling. In combination, our existing tools, training policies, and production requirements perpetuate the "cut and paste" syndrome. This is all part of a broader national failure, my final concern.

The six sins discussed above come together in our failure to develop a national knowledge management strategy and a related national information technology strategy. We spend too much on classified collection which we cannot process in time, and not enough on open source information, including foreign scientific and technical literature vital to our national competitiveness. We have done well at linking a vast array of different computer databases and capabilities, but at a huge cost in terms of people and maintenance dollars, and without significantly improving the individual analyst's access to data. We have failed completely at developing a standard advanced analysts' toolkit (workstation with integrated application), and we are therefore wasting millions building hundreds of different workstations and application packages which provide slightly different implementations of the same generic functionality at thousands of sites throughout the world.

In short, we have done nothing to improve the quality of life for our individual analysts, and little to improve their intellectual reach. In a broader context, outside the intelligence arena, we have failed to use federal funds in the knowledge management arena to support, direct, and synergize private outlays in the commercial and academic sectors. Our nation is significantly behind its potential in exploiting the available knowledge in the world, and the available information technologies, and this is a "grand strategy" failure of enormous proportions. Within intelligence, we will continue to have strategic failures so long as we continue to intellectually shackle and starve our diminishing population of analysts by failing to act in the two areas offering very significant returns on investment: the integration of now-operational advanced information processing technologies into a single standard analysis "toolkit" exportable to any enterprise; and the development of a multi-level and multi-media database architecture which seamlessly merges classified and unclassified data, and extends the analyst's reach to every corner of the globe.

As an aside, let me note my support for those initiatives sponsored by the Federal Coordinating Council for Science, Engineering, and Technology ("Grand Challenges: High Performance Computing and Communications"), and the related "computer superhighway" concepts coming off the Hill. Both reflect our national tendency to focus on "big problems" and "technical solutions". Where my emphasis differs from these two major initiatives, in a complementary way, is through my focus on "enabling tools" which give large numbers of people greater access to data, rather than great computing power to a few select scientists and their acolytes.

What is to be done?

(1) Adopt David Abshire's idea of an Advisor to the President for Long-Term Planning, and make that individual the Presidential champion of a national knowledge management strategy, work-

ing in concert with the Office of Science and Technology Policy and other interested parties.

(2) Establish a Senior Inter-Agency Group (SIG/C4I) tasked with directing resources toward a global C4I system that provides multi-level security access (to include foreign nationals with no clearances), integrates multi-media databases, and establishes a standard advanced analysis "toolkit". The Information Handling committee (IHC) and the Advanced Intelligence Processing and Analysis Steering Group (AIPASG) should serve as focal points for inter-agency coordination while the SIG/C4I provides a decision-making forum and ensures that the external investments in communications and unclassified computing are part of an integrated continuum of government-private sector spending. Use the Defense Information Systems Agency (DISA), the Intelligence Communications Architecture (INCA) Project, and the Joint National Intelligence Development Staff (JNIDS) as executive agents for implementing a national knowledge management campaign plan. Have the new Advisor to the President for Long-Term Planning chair this group, with an assistant to serve as Executive Secretary.

(3) Use the Corporate Information Management (CIM) initiative to begin exploring inter-agency solutions and mechanisms for fully integrating open source and unclassified databases into a global C4I architecture. Provide a mechanism for conveying to Comptrollers the evaluations and recommendations of the IHC and AIPASG as a means of accelerating the retirement of inefficient installed bases while consolidating resources to attack generic problem sets. In particular, end the isolation of intelligence systems from all other C4 systems - C4 must improve its personnel security levels and adjust its approach to accommodate intelligence, but intelligence systems managers must understand that their days of pipeline management and compartmented resource allocation are over.

(4) Establish a new National Information Agency (NAI) which folds in the National Technical Information Service (NTIS) of the Department of Commerce, the Foreign Broadcast Information Service (FBIS), the Joint Publications Research Service (JPRS), the Defense Gateway Information System (DGIS), and the Defense Technical Information Center (DTIC), while also folding in and revitalizing the Federal Research Division of the Library of Congress, and creating a new consolidated joint government-business Center for the Exploitation of Open sources (CEOS). Such a national investment could be fruitfully directed to:

(a) Engage in "competitive analysis", using only open sources, as a means of challenging the assumptions of the remainder of the intelligence community regarding the value of extremely expensive and fragmentary classified sources; and

(b) Emphasize direct support to national and private research endeavors, with a view to stimulating and reinforcing business and academic research and development in all domains.

(5) Establish an Open source Committee under the Director of Central Intelligence, to serve as a focal point for intelligence community collection and processing of open source information (which would include multi-spectral imagery as well as public signals, unclassified documentation, and open debriefings and interviews). Utilize military intelligence personnel and capabilities in peacetime to "jump start" the open source collection and exploitation process - this will help the military because many of the Third World intelligence gaps stemming from our obsession with the Soviet Union can be filled relatively quickly through systematic, legal, and overt access to unrestricted foreign information.

(6) Consider reorganizing the Central Intelligence Agency to provide for four distinct capabilities: a national intelligence analysis capability with nu-

merous inter-agency collection management and analysis centers along the lines of the existing centers focused on special topics; a consolidated clandestine operations agency with its own communications and computing capabilities but integrating tactical SIGINT, necessary technical support and a new separate Office for Military Contingencies manned jointly by military and civilian personnel; a national technical intelligence agency to manage overhead technical collection systems; and finally a national intelligence research and development (R&D) agency under a new deputy director responsible for consolidating and managing the now fragmented intelligence R&D efforts scattered among different services and agencies.

...the vast outpouring of multi-media, multi-lingual knowledge has presented us with an enormous technical and intellectual challenge...

Knowledge is power. Technology has broken down the walls that previously required vast technical and human endeavors to isolate nationally vital information about plans, intentions, and capabilities. At the same time, the vast outpouring of multi-media multi-lingual knowledge has presented us with an enormous technical and intellectual challenge, one worthy of the same kind of national attention occasioned by past energy crises. There is still a role for clandestine human collection and covert technical collection, but it must be more tightly focused. Our emphasis must shift from collection to analysis, from indiscriminate collection to integrated processing, from analysts as assembly-line producers chained to their desks to analysts as observers and partners in the national decision-making process - not making policy, but informing policy.

Finally, we must shift away from a strategy of producing highly classified compendiums of information for a few select customers, and toward maximizing public access to basic knowledge in all areas of endeavor.

The sins of intelligence will always be with us in one form or another;

restructuring will cure some ills and bring on others; our greatest challenge continues to be one of strategic vision - if we can change the way we view analysts and their role in the daily decision-making process; if we can adopt a national knowledge management strategy, accelerate our integration of national C4I systems, and address the open source chal-

lenge; then we will have accomplished a far more fundamental and constructive "restructuring" - applied a "new paradigm". This strategic interpretation is consistent with the present restructuring plans, but of far greater import to how our Nation "does business" in the future.

THE NATIONAL SECURITY ACT OF 1992

by Robert David Steele



Mr. Steele has served in a variety of assignments on both the military and civilian sides of the intelligence community. He currently is a special assistant to the Director of Intelligence, Headquarters USMC, involved in planning, resource analysis and programming. He is also a dynamic and highly productive volunteer Assistant Editor of the Journal and the organizer of an Open Source Information Symposium supported by NMIA. The comments that follow reflect personal views and do not represent the policies or positions of any government organization or this Journal.

As we pass through the ides of March, we have in hand two bills (proposed laws), one from Senator David Boren, Chairman of the Senate Select Committee on Intelligence (SSCI), the other from Congressman Dave McCurdy, Chairman of the House Permanent Select Committee on Intelligence (HPSCI). Both bills, S.2198 and H.R.4165, are intent on reorganizing the United States Intelligence Community.

Both bills are widely perceived primarily as a means of airing the need for specific changes without necessarily requiring passage of the bills as now offered. The bills reflect legitimate concerns about the effectiveness of our existing structure, and we have no alternative but to respond with thoughtful documented views on why or why we do not need to modify the way we do business.

On that note, what follows is a brief examination of major elements in the two bills, together with a commentary which includes proposed modifications or additional elements.

One comment that can be made in relation to DNI authorities (figure 1) is that Executive Order 12333 already authorizes the DCI to review and approve National Foreign Intelligence Program (NFIP) reprogramming requests, and to levy tasks and develop guidance. There is something to be said for divorcing the DNI from the Central Intelligence Agency (CIA), if a truly "joint" civilian-military inter-agency staff can be established. A career at CIA, or service as DCI, should not be considered essential qualifications for the role of DNI, nor should a change in the DNI's authority to undermine the role of the Secretary of Defense in training, organizing, and equipping military intelligence forces be allowed to occur.

An obvious question that occurs to one contemplating the changing definition of national security and the

- Director of National Intelligence (DNI)**
S: Creates separate position from that of Director, Central Intelligence Agency
H: Same
- DNI and the National Security**
S: Makes DNI a non-voting member
H: Same
- DNI and Military Representation**
S: Either DNI or Deputy DNI must be active or retired military officers (four star)
H: DNI may not be an active duty officer
- DNI Authority**
S: Provides DNI with authority over collection priorities, funds, and personnel throughout the intelligence community
H: Similar, more pointedly stated

Figure 1. Director of National Intelligence

growing importance of foreign commerce and fiscal issues as well as environmental, energy, and medical threats is: why not also make the DNI a non-voting member of the Council of Economic Advisors?

Intelligence Producers Council, and of course the President's Foreign Intelligence Advisory Board, must wonder if a different group, and particularly one so senior, will have the time or inclination to set the house in order.

counterterrorism, counterintelligence, and counternarcotics all appear to have been highly successful. There will be a need for balance between consolidated inter-agency analysis capabilities, and distributed consumer-driven in-house analysis capabilities; one might draw the analogy that the inter-agency centers are akin to the Joint Intelligence Center, while the Departments must each retain a cadre of on-site analysts. There is no substitute for organic Departmental capabilities, a requirement both bills recognize in mandating Departmental capabilities for the military (but not for the civilian elements of the community nor the consumers not traditionally included in the community).

- **NFIP Management**

S: DNI gets the money, not the Departments; breaks NFIP out as separate budget line

H: Same but requires total budget (not budget detail) be released as unclassified figure

- **Priorities Management & Evaluation Oversight**

S: Creates Committee on Foreign Intelligence within National Security Council with NSC principals or deputies as members; responsible for priorities, requirements, and evaluation; includes Commerce

H: Similar without evaluation function

- **Intelligence Evaluation Board**

S: Creates independent board under DNI

H: Same

Figure 2

Someone should be in charge (figure 2), but we must avoid legislation which gives total control of all intelligence monies to an individual or organization (in the generic sense) still focused on the "top 100" policy-makers and relatively oblivious to the distinctions between Departmental and Service policy, planning, and programming authorities; theater commander and Country Team members; tactical commanders and humanitarian assistance organizations; and technical systems developers, to include those responsible for environmental, energy, and medical issues. Cabinet members in particular must, as both consumers and producers, increase rather than reduce their role in the management of national intelligence resources.

The idea of having customers establish priorities and requirements, and evaluate production, is a good one, but one familiar with the existing Foreign Intelligence Priorities Committee, the Future Intelligence Requirements Working Group, the National Intelligence Topics effort under the auspices of the

On balance these ideas merit discussion, but until they are reinforced with a clear-cut concept for ensuring that customers in every government agency, at every level of operation (strategic, operational, tactical, and technical) have an established basis for obtaining timely and useful intelligence support, then the Committee runs the risk of being one more "pro forma" means of pandering to the top-level individuals while the broader customer groups starve to death.

The Intelligence Evaluation Board under the DNI has tremendous potential if it could actually *do* program evaluation and not go through the motions of conducting surveys. To be credible the results of the evaluations must at a minimum be available to all consumer principals including Department and Service chiefs, Commanders-in-Chief of the theaters, agency heads, and Ambassadors.

The propositions reflected in figure 3 are provocative and thoughtful. The prototype inter-agency centers for

There are related new ideas emerging from such groups as the Advanced Information Processing and Analysis Steering Group, and associated analyst advisory groups. We may yet see the Army's Scientific and Technical Liaison Office (STILO) concept considered as a model for providing direct face-to-face analyst support to every customer, with the liaison analysts in turn drawing on integrated databases as well as direct tasking capabilities for both ad hoc production by analyst teams, and ad hoc collection.

There are two major shortcomings in both House and Senate bills, and that is the failure to address the need for a Deputy DNI for Communications & Computers (Deputy DNI (C&C)), as well as a Deputy DSNI for Research & Development (Deputy DNI (R&D)). It simply will not be possible to support an inter-agency analysis and collection management environment without a Deputy DNI (C&C), and it will not be possible to get the scattered R&D budgets under control, and channeled toward maximizing the productivity of our dwindling inter-agency personnel base, without a Deputy DNI (R&D).

The system has become the product. This is a simple concept, but it is not well understood by most managers. As we move toward near-real-time processing of multi-media information, and

- **Deputy DNI for the Intelligence Community (IC)**
S: Creates position, in lieu of the existing Director, Intelligence Community Staff
H: Similar, requires Deputy DNI(IC) to be military flag officer
- **Deputy DNI for Estimates and Analysis (E&A)**
S: Creates position to foster inter-agency analysis & estimates capabilities
H: Similar, precludes Deputy DNI (E&A) from being a military officer
- **National Intelligence Council (NIC)**
S: Provides statutory basis for existence as a collection of senior community advisors
H: Same
- **Office of Intelligence Analysis**
S: Provides for integration of CIA analysts and analysts from other agencies into one office
H: Same
- **Office of Open Source Information**
S: Not addressed
H: Creates a new community-wide office under Deputy DNI (E&A), to procure, coordinate, and disseminate open source intelligence
- **Office of Warning and Crisis Support**
S: Creates new community-wide office under Deputy DNI(IC) to focus on potential threats, identify action options, and provide crisis support to policy-makers
H: Same, without focus on action options
- **National Intelligence Center "campus"**
S: Requires DNI and both Deputy DNIs to sit in same building, to be called the National Intelligence Center
H: Provides for DNI but not Deputies

Figure 3. Major Analysis Initiatives

as our dissemination networks gradually develop a rapprochement with their over-capitalized collection networks, two things are going to happen: the consumer is going to insist on inter-active access to the databases, and the death knell will sound for most hard-copy products. Right now, despite recognized advances in technology, the systems design and product planning processes are completely divorced, there is no ability to plan multi-media product families, and there is no real integration of system or product planning between agencies and disciplines.

One obvious "tag" that must be imposed on all collection is that of time and space. The Navy does this very well with aspects of its signal intelligence. A second obvious foundation that is needed—the third layer, if you will—to permit a true merger of system and product, is that of integrated digital mapping data. A consumer should be able to "drive" or "fly" around the world, zooming in as required. There is no finer intuitive database management structure than that provided by a global map against which all relational databases can be grounded. One superb demonstration of how this will change the way analysts

examine data has been developed by The MITRE Corporation through its Open Source Processing Research Initiative, elements of which are based on original work done by the USMC Intelligence Center in response to consumer demands.

In short, the four Deputy DNI's should respectively and collegially represent consumers (IC), production (E&A), dissemination (C&C), and strategic planning (R&D).

There are (figure 4) three kinds of HUMINT: clandestine, covert, and overt. Although it possesses capabilities to accomplish all three, the CIA is best at just one—clandestine—and then only when priorities permit the full application of resources, to include sufficient personnel to allow a proper case office to agent ratio and the full exploitation of tradecraft. There have been significant improvements in the past decade, in both clandestine operations and covert operations such as were executed in Afghanistan and are now supporting law enforcement in its war on drugs. There has been some attention to the need to improve overt capabilities, but the full value of this global resources base is not yet fully appreciated. Incremental changes in these areas will not be sufficient to prepare us for the challenges of this decade, much less the catastrophes of the next. We must have nothing less than a "total make-over" in all three areas.

For this reason direct military augmentation of the CIA's Directorate of Operations, both through long-term assignments of military case officers, and a long-term program to recruit and maintain a cadre of Department of Defense (DoD) civilian case officers is useful.

Since military contingency operations and stay-behind operations do not require the kind of sensitive and ongoing tradecraft and reporting requirements that characterize political and economic targeting, much increased utilization of third country "career agents" and ethnic U.S. citizens who might not otherwise be eligible for clandestine assign-

- **Director, Central Intelligence Agency**
 - S: Provides for separate individual in this position while essentially restricting responsibilities to clandestine operations, covert action, and global services of common concern (e.g. secure communications)
 - H: Same but apparent contraction with conversion language in establishing DNI from DCI position
- **Assistant Deputy Director of Operations (Military Support) (ADDO(MS))**
 - S: Establishes new military flag officer position intended to serve as liaison to Department of Defense clandestine human intelligence (HUMINT) capabilities, while extending 's authority to all HUMINT capabilities in community
 - H: Not addressed

Figure 4. HUMINT Initiatives

ments should also be stressed. Long-term non-official cover "residents", some with direct action capabilities, must also be established. We must do much, better at maintaining truly clandestine networks which are impervious to curfew and responsive to our needs for both early warning and pathfinding.

Covert HUMINT is a special operations matter, and requires committed and specially trained military personnel. Given the very genesis of CIA's capability in the militarized Office of Strategic Services, there is a good case to be made for putting the CIA's paramilitary and psychological warfare capabilities under the direction of the Commander-in-Chief, U.S. Special Operations Command (USCINCSOC), with a senior CIA officer as a civilian deputy. Alternatively, CINCSOC or his civilian CIA deputy could be designated ADDO for Covert Action, thereby preserving a special relationship with the DCI and the DDO.

There are competing views on this matter. One view holds that the real value of the traditional intelligence community is its ability to *take action* and to discreetly make arrangements not amenable to public diplomacy. The foundation of discretion is tradecraft, and for this reason it *may* be essential to leave

the clandestine and covert services of the CIA under one leader. If so, some sort of Memorandum of Agreement is probably required between USCINCSOC and the DCI, one which provides tradecraft augmentation to special operations forces when required, while keeping the CIA out of the paramilitary business above the squad level. Alternatively, there must be much close coordination between USCINCSOC personnel and those responsible to the DCI for covert operations.

In either case, we should reinforce the ability of the Department of State to support public diplomacy and

overt action by private groups where deemed appropriate. This will be critical to our future success in the "cultural wars" which Bill Lind, among others, has predicted.

Overt HUMINT will never be properly handled by people whose culture not only denigrates "unclassified" information, but also devalues and restricts dissemination and exploitation of the information by imposing all kinds of handling restrictions associated with *who* collected the overt information, not *what* the information conveys.

The idea of integrating management of clandestine HUMINT capabilities as well as overt capabilities such as our superb defense attache system therefore causes concern. As it is, too many clandestine case officers are spending too much time collecting routine political and economic information which representatives of other organizations would collect overtly if they had the representational funds and language skills they required; at the same time, for lack of responsiveness from that same clandestine cadre, organizations with overt assets may be tempted into indiscretions out of frustration.

Integrated management of clandestine capabilities, and significant military reinforcement of those capabilities, is called for, but overt capabilities should be under the operational direction of a

- **Defense Technical Information Center**
- **Federal Research Division, Library of Congress**
- **National Technical Information Service**
- **Foreign Broadcast Information Service**
- **Center for the Exploitation of Open Sources**
- **Office for Multi-Spectral Digital Information**

Figure 5. National Information Agency

non-intelligence activity which provides overt collection management services.

This is a reason why the House initiative for an Office of Open Source Information is of interest. We need a National Information Agency (NIA) which is independent of the intelligence community and able to provide direct support not only to the government, but to the private sector in the latter's role as an element of national competitiveness.

Such a capability can readily be built around the Defense Technical Information Center (DTIC) with DoD as the executive agent for open source intelligence; and be expanded to integrate the Foreign Broadcast Information Service (FBIS) of the Central Intelligence Agency, the National Technical Information Center (NTIS) of the Department of Commerce, the Federal Research Division (FRD) of the Library of Congress, and a new Office for Multi-Spectral Digital Information.

This new national activity, independent of but responsive to the needs of the intelligence community *and all other government Departments*, may merit its own program line—in the same manner that Congress was forced to create Program 11 to ensure proper attention to special operations and low intensity conflict, Congress may well have to create Program 12 (Consolidated Open Source Program) to establish the foundation for our national knowledge management (and knowledge warfare) capabilities of the future.

There is another aspect of open source exploitation which the bills do not address, and may not need to address, but which must assuredly be considered within the executive branch: the privatization of basic encyclopedic intelligence.

Between the flood of available unclassified information, the dwindling (and sometimes unsuitable) classified collection and analysis capabilities, and the common concern in government and

private sector over national competitiveness, there is every reason to create a National Knowledge Foundation (NKF) whose purpose is to foster a joint government-private sector endeavor establishing a national open source architecture.

A Center for the Exploitation of Open Sources (CEOS) affiliated with the NIA and managing NKF funds would help achieve this objective and have the added advantage of not be constrained in providing direct support to national enterprises and academic institutions.

The above could be readily included in the Program 12 budget, with legislation (or a separate Executive Order) ensuring that these capabilities are carefully integrated with the existing National Education & Research Network, while also ensuring oversight necessary to protect both civil liberties and proprietary equities.

Communications and computing are showstoppers in the intelligence business, and every other business (figure 6). There is much to be said for having a separate ASD(I), but only—and

this must be stressed—if there is an ASD(C³) and they are both under the same senior manager, i.e. a new Undersecretary of Defense for C³I. Given the great importance that must play as we gear up for computer warfare, precision targeting, non-proliferation raids, and so on, there are very powerful reasons for increasing the level of representation for intelligence within DoD. On the other hand, the existing DoD arrangement in which the ASD(C³I) has direct access to the Secretary appears to be working very well and appears to provide the necessary means for obtaining top-level direction and attention.

More important than the bills' focus on the idea of an ASD(I) is the *lack of attention by the bills to the level of representation which intelligence does or does not receive in the other Departments of government*. It would not be unreasonable to use the proposed National Security Act of 1992 to negotiate with each Cabinet member the level of representation and the percentage of resources to be devoted to meeting their intelligence needs for the remainder of this century.

- Assistant Secretary of Defense for Intelligence (ASD(I))
 - S: Establishes this position to serve as focal point for accountability; in this way provides for the de facto integration of programming and budget oversight functions in relation to NFIP and Tactical Intelligence and Related Activities (TIARA) resources
 - H: Does not establish position; does require Secretary of Defense to ensure TIARA complements NFIP, and to establish a Consolidated Defense Intelligence Program (CDIP) within NFIP
- Military Departments
 - S: Provides statutory basis for intelligence capabilities of the military departments, and distinguishes between the needs of military planners, tactical commanders, acquisition managers, training and doctrine needs, and research & development.
 - H: Similar

Figure 6. DoD Departmental Initiatives

- **Defense Intelligence Agency (DIA)**

S: Provides statutory Basis and sets forth expanded duties and responsibilities; Director appointed by Secretary in consultation with DNI; term of four years

H: Same

- **National Security Agency (NSA)**

S: Provides statutory basis and significantly expanded authority including operation of unified national capabilities, and responsibility for procurement and operation of national signal intelligence (SIGINT)

H: Supports unified operations, but creates separate Reconnaissance Support Activity (RSA) in DoD to be responsible for R&D, procurement, and operation of national systems

- **National Imagery Agency (NIA)**

S: Creates a new organization responsible for procuring and operating national imagery systems as well as managing a unified imagery program including airborne platforms, analysis, and dissemination

H: Same, but RSA would function as with NSA

Figure 7. Defense Agency Initiatives

The historical differences between the intelligence committees and the armed services committees could be strategically diffused if committees dealing with the other Departments of government were made full partners in the intelligence restructuring and management process. As we shift from the industrial era to the knowledge era, increased investments in intelligence will be necessary, and only possible if other Congressional elements are fully involved.

These initiatives (figure 7) appear flawed. It is essential for all concerned to understand that both NSA and DIA are designated Combat Support Agencies within the National Defense Reorganization Act of 1986 (Goldwater-Nichols) and therefore responsible to the Secretary of Defense and the Chairman, Joint Chiefs of Staff.

The National Imagery Agency, because of the diminution of the need for strategic targeting data against denied areas, and the continued critical short-

falls in precision targeting and basic mapping data for the Third World, should incorporate all or part of the Defense Mapping Agency, and called the National Imagery and Mapping Agency.

This agency, especially if built around an existing DoD agency, should be designated a Combat Support Agency.

The provisions or concepts in the two bills do offer significant prospects for improving our national and defense intelligence capabilities, assuming a DNI and Deputy DNIs with a full appreciation for consumer needs beyond the inner circle of the "top 100" policy-makers.

This is not to say that the passage of legislation is the means by which to achieve the agreed upon objectives. The bills place great reliance on a strong DNI, and presume the DNI and his or her immediate staff will have the vision and breadth of understanding necessary to meet the strategic, operational, tactical, and technical intelligence needs of all of the Departments of government.

The process would be improved by a stronger evaluative and resource management role played by the lower-level consumers of intelligence, or a legislatively protected distribution of analysis capabilities, together with an accompanying increase in resources devoted to collection, analysis, and dissemination

- Mandate DNI role as non-voting member of the Counsel of Economic Advisors
- Modify Committee on Foreign Intelligence charter to integrate representatives from every department at each level of operations
- Require an annual report from the Intelligence Evaluation board to Congress as a whole
- Establish a minimal mandatory funding and manning level for each Department's internal intelligence, communications, and computing capability
- Establish two additional Deputy DNI positions, one for C&C and one for R&D
- Establish increased participation by the Congressional committees responsible for other departments of government, with a view to increasing oversight over performance against non-conventional targets

Figure 8. Recommended Management Adjustments

- Add a Military Support Division to the CIA's Directorate of Operations, manning this element with military and DoD civilian personnel
- Transfer the CIA's covert action elements to the operational control of USCINCSOC, with a senior CIA officer as deputy for covert action, or execute MOA between DCI and CINC
- Establish a National Information Agency with DoD as executive agent, DTIC as the foundation, and integrating FBIS, NTIS, FRD, and two new centers, one for joint endeavors with the private sector, the other to deal with multispectral imagery requirements and production
- Expand the proposed National Imagery Agency to integrate the Defense Mapping Agency and form a new National Imagery & Mapping Agency

Figure 9. Recommend Operational Adjustments

capabilities necessary to deal with non-conventional and emerging threats and circumstance.

Below (figures 8 & 9) are summaries of recommended modifications to the bills as now being circulated, providing a contribution to the constructive dialogue that must be pursued between the legislative and executive branches as we adapt to our changing circumstance.

In the operational area, the focus has been on significantly reinforcing the CIA's clandestine operations capability, transferring the covert action capability to CINCSOC, establishing a separate national open source capability, and ensuring that any national capability for imagery pays due heed to our mapping shortfalls. In addition, there is a need to have DDNI's specifically charged with integrating communications and computing, and research and development, across organization boundaries; and a further need to expand the Congressional committee base from which support for increased investments in intelligence can be obtained.

In addition to the above recommendations that respond directly to the content and intent of the two bills, there are several major areas where neither the

bills nor the executive restructuring efforts venture, areas that are essential to making the organizational changes, whether achieved by law or executive order, meaningful and truly effective.

All too frequently, those engaging in these exercises forget to ask the fundamental question: *who is the customer?* Even those that do ask this question fail to appreciate the gamut of distinct customer groups. Implicitly, failing to recognize all customers is antithetical to our on-going efforts to increase jointness and interoperability, not only between the military services, but between the military and law enforcement, between our forces and those of foreign organizations, and between civilian government agencies not now full participants in the national and defense intelligence process.

Answering the question "who is the customer" is also a good means of scrutinizing the basic terms of reference—what is the objective of intelligence analysis? To what end do we maintain a multi-billion dollar capability? Defining the customer also helps to define the enemy, or target; as the customer changes, so does the target. Overlooking certain customers virtually assures blindness in some areas, and commensurate intelli-

gence failures. We are in the midst of a metamorphosis.

Who is the customer? What do they need? how do we ensure they get what they need? These are issues which we have not considered as fully as we should in our executive restructuring efforts, and which are also not adequately addressed in the proposed legislation.

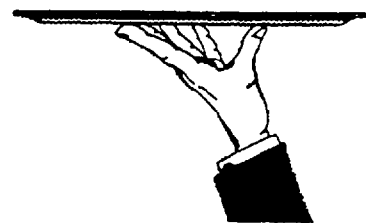
When you get right down to it, most of the players still appear to be thinking about block and wire diagrams and funding authority, when they should be thinking about truly changing the way we do business by substantially expanding the customer base for intelligence, redefining our national security concerns, integrating the individual analysts into the daily lives of their customers, and recapitalizing our infrastructure to take full advantage of the rapidly expanding sources of unclassified information, while also empowering our dwindling work force.

We must come to grips with these basics if we are to really improve our national security and national competitiveness.

**Make your
NMIA Awards Banquet
reservations**

NOW !

**Call Gerry Stowe
(703) 821-3200**



Intelligence Support for Expeditionary Planners

Planning for the type of threats we're likely to encounter in an expeditionary environment and making information about these threats and the places they emanate from readily available to users in the Fleet Marine Force is one of the main taskings of the Corps' new Intelligence Center. The article below looks at how the Center is bringing national-level intelligence assessments down to the field commander in a timely fashion—in some cases even before a contingency arises.

by Robert D. Steele

In 1987 then-Commandant Gen A. M. Gray directed the establishment of the Marine Corps Intelligence Center because he recognized a critical shortfall in mid- and long-term intelligence support to Service doctrine, training, and acquisition policy and programming. It fell to Col Walter Breede, the founding director, and later Col Forest L. Lucy, who is the current director of the Center, to implement the Commandant's vision. As special assistant to the director, I worked closely with both towards this goal.

We approached our mission with the shared conviction that national and defense intelligence production communities today do not have a proper framework within which to meet the needs of Service planners. After some reflection we identified five areas we had to focus our efforts on in order to prepare tailored intelligence

for our Marine Corps customers. These five areas include (1) the classified nature of intelligence material available today; (2) the type of expeditionary environment Marines are likely to encounter while deployed; (3) mission-area factors likely to influence a Marine deployment; (4) the level of analysis used to shape the intelligence estimate; and (5) the danger in overgeneralizing about specific areas of interest. These five areas are discussed below.

Level of Classification

One of the most difficult problems to overcome when trying to get intelligence to the field is the issue of classification. What the problem boils down to is simply the greater the classification, the less useful the product is to the people who need it most. A corollary to this is the longer the document, the less likely it is to be read. In order to overcome this problem, an unclas-

WESTERN HEMISPHERE	MIDDLE EAST/ SOUTHWEST ASIA	AFRICA	ASIA/ PACIFIC	EUROPE/ MEDITERRANEAN
Argentina Bolivia Brazil Colombia Costa Rica Cuba Dominican Republic El Salvador Grenada Guatemala Haiti Honduras Jamaica Mexico Nicaragua Panama Peru Suriname Venezuela	Bahrain Egypt Iran Iraq Israel Jordan Kuwait Lebanon Libya Oman Qatar Saudi Arabia Syria U. Arab E. Yemen	Algeria Angola Djibouti Ethiopia Kenya Liberia Madagascar* Morocco Mozambique Namibia Somalia S. Africa Sudan Tunisia Uganda Zaire Zimbabwe	Afghanistan Bangladesh Brunei Burma Cambodia India Indonesia Japan Laos Malaysia N. Korea Pakistan Papua N.G. Philippines PRC (Coast) Hong Kong Taiwan Singapore S. Korea S. Pacific** Spratly Is.*** Sri Lanka Thailand Vietnam	Denmark Greece Italy Norway Poland Turkey Yugoslavia
19	15	17	22	07

- * Includes Seychelles and Mauritius
 ** Includes Fiji, Kiribati, Vanuatu, New Caledonia, Solomon Is., and the general vicinity of Australia and New Zealand
 *** Claimed by seven nations

Table 1: Expeditionary Environment Watchlist

Ground Overview Infantry Artillery Armor C4I2 Support Service Support Leadership, Training, and Readiness Military Manning Military Manning Foreign Advisors Contractors Reserves Parasilitary/ Special Ops/ Elite Guards	Combat Support Anti-Tank Engineers Military Police PsyOp & Civil Affairs Service Support Supply Maintenance Transportation Readiness Plus Leadership Training Maintenance	C4I2 C2 and Comms Computers Intelligence & Inter- operability EW Support Measures (ESM) Countermeasures (ECM) Counter-counter- measures (ECCM) NBC Nuclear Chemical Biological Delivery	Aviation Overview Air Surveillance Weapons Support Fighter Aircraft Fixed & VSTOL Strike Aircraft Fixed & VSTOL Helicopters (Air & Trans) Surface to Air Missiles Anti-Aircraft Artillery Air to Air Missiles Reconnaissance Airborne Early Warn/Control Tactical EW Training & Readiness
---	---	---	--

Table 2: Military Factors

THREAT	MISSION AREA: ARTILLERY
HIGH:	Self-propelled or towed, with rockets & missiles, NBC, range 30K+
MEDIUM:	SP or towed, with some missiles, bio-chem, less than 30K range
LOW:	Towed artillery with less than 30K range and/or mortars

Table 3: Mission Area Threat Definitions

sified global overview document was developed that could be used as a basic reference for planners and students throughout the Fleet Marine Force (FMF). This guide, it was felt, could provide field commanders general but useful data on a particular area they were interested in, without burdening them with stringent classification processes. This resulted in various country reports that emphasized conclusions and obscured the sourcing and detail supporting those conclusions. The supporting documentation, at higher levels of classification, would still be available to customers, but the country reports would be more readily available for wide distribution because of their lower classification.

The Expeditionary Environment

Our customers need tailored products that take national intelligence products and turn them into concise, usable products of immediate value to Marines. This suggests the need to couch our intelligence reports in relation to countries and mission areas of greatest importance to the Marine Corps. Therefore, it was decided the Marine Corps needed to create a list of countries where Marines were most likely to be employed.

The early list, based on queries to G-2s, consisted of 67 countries and 2 island groups. Our most recent list, reflecting the consensus of many general officers, consists of 80 countries in 4 different priority categories. The current plan is to update the list annually and distribute it throughout the FMF upon acceptance by the Commandant.

Table 1 lists the countries on the 1991 list. This list is important for two reasons: First, it provides a basis for evaluating the degree to which our needs are being met. Are our attaches in the right countries? Do we have 1:50,000 maps for our most important countries? Are national intelligence collection capabilities able to monitor emerging threats in a given area?

Second, it provides a basis for developing strategic generalizations vital to Service acquisition policies. Is our standard aviation day "hot" rather than "warm"? Are bridges in a specific country able to handle more than 30 to 40 tons on average? If many countries on the list have no usable po-

BASIC TOPOGRAPHY	GROUND ASSAULT	ASSAULT HYDROGRAPHY	AERONAUTICAL CONDITIONS	OPERATIONAL INFRASTRUCTURE	BASIC WEATHER
Surface Configuration	Cover	Beaches	Ops Elevation	Port Access	Temperat.
Surface Vegetation	Concealment	NGF (5 fathom line)	Aerial Visibility	Port Utility	Windspeed
Surface Materials	Inter-Visibility	Surf Conditions	Aerial Ceiling	Air Terminals	Precipit.
Surface Hydrology	Landing Zones	Approach Conditions		Road/Rail Net	Humidity
Man-made Features	Drop Zones	Riverine Network		Bridges	Light Data

Table 4: Operational Geography

POLITICAL	PSYCHOLOGICAL	ECONOMIC	INFRASTRUCTURE	NATURAL RESOURCES
Allies	Religion & Language	Strikes & Riots	Key Facilities & No Fire Areas	Contiguous Hostile Area
Opposition	Group Divisions, Customs/Taboos	Black Market, Corruption, & Mil/Pol Crime	Urbanisation & Population Issues	Water Supply
Intelligence	Myth/Identity, Media Themes, & View of USA	Unemployment & Inflation	Disease & Public Health Resources	Food Supply
Government	Education	Basic Civilian Staples/Supply	Public Voice/Print Media & Telecommunications	Energy Supply
Human Rights	Intellectuals	Garrison State	Public Works (Power & Water)	Strategic Minerals & Raw Materials
Public Form, Franchise, & Opinion	Censorship	Foreign Capital & Capital Flight	Public Transportation Assets	Production Base
Legal Codes	Violence	R&D Program	Electronic Computing & Storage	Land Tenure

Table 5: Civil Factors

facilities, have we made provision for this in our sustainability planning? If most capital cities are beyond the round-trip range of a CH-46 flying from the five-fathom line, what does this mean to noncombatant operations?

Mission-Area Factors

With assistance from the Warfighting Center at Quantico, we began developing a framework for analyzing these various countries in terms of military capabilities. A list of the various capabilities that we looked at is included in Table 2. Note that each major mission area can be broken down into more detailed categories, each of which is defined in terms of the level of threat—high, medium, and low—it represents to a force operating in a given area. Table 3, for example, shows how a mission area such as artillery could be ranked.

Military capabilities, however, were not enough. Too often our most experienced professionals forget the importance of terrain intelligence and civil factors. Consequently, we developed matrices for these factors as well (see Tables 4 and 5).

The importance of the terrain in each country under study could not be dismissed. Terrain affects a host of other considerations—from what type of equipment you need to what kind of concept of operations you employ. But the “threat” could not always be counted on to be encountered on its “home” terrain. For example, country X’s ground order of battle, in the case of an invasion or a foreign adventure like Cuba in Angola, should be evaluated in relation to both its home conditions and conditions in countries where it might be encountered.

In the case of civil factors, we not

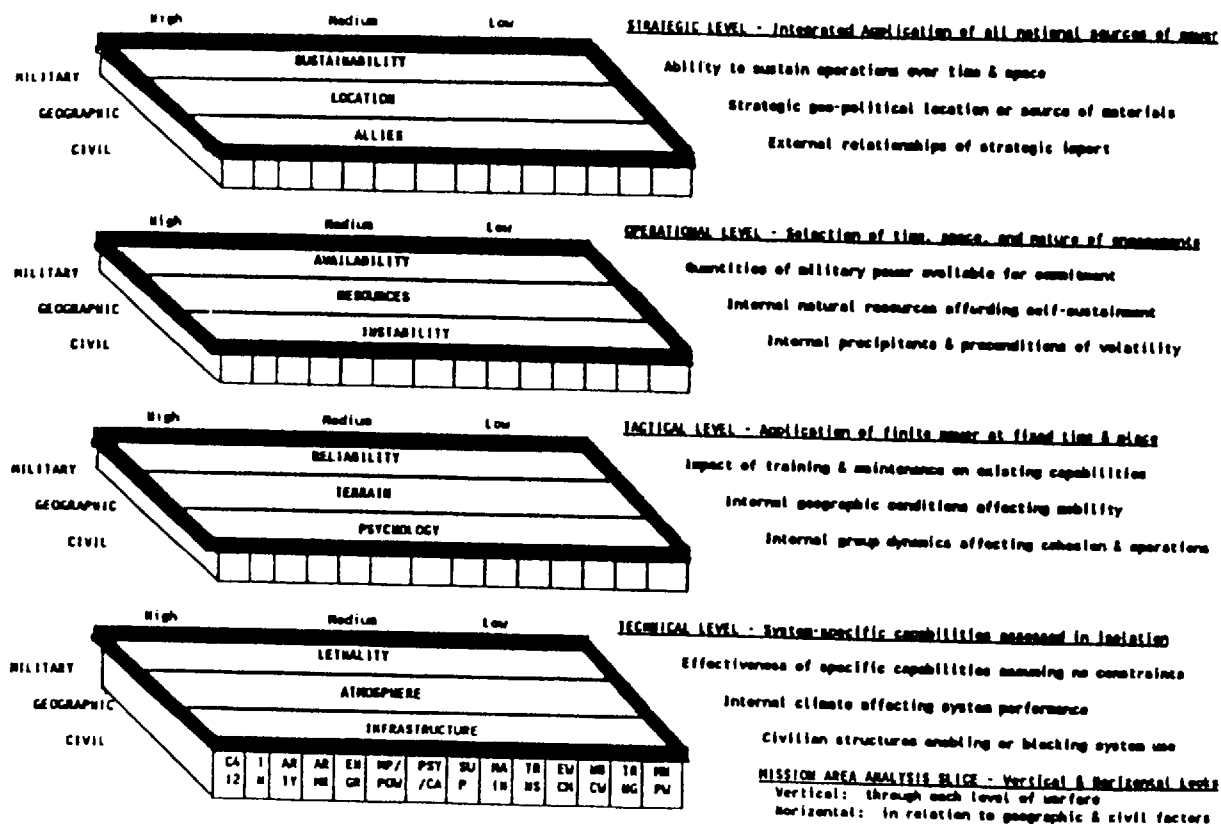


Table 6: Levels of Analysis

only answered the "so what" question for each factor included in our model, but also distinguished between those factors of greatest importance during short-term operations (top two rows), mid-term operations (second tier), and sustained operations (lowest tier). We then cross-referenced our civil factors against the factors identified by the Army-Air Force Center for Low-Intensity Conflict, which is now using our model as a building block for its own efforts.

Level of Analysis

Over a year ago we scrubbed our initial model by inviting the top analysts for a specific Middle Eastern country from throughout the national and defense intelligence communities to spend a day testing each factor and each definition against a certain country. We very quickly discovered that the threat changes depending on the level of analysis (see Table 6).

Taking tanks as an example: At the technical level, a given country can be a very high threat because it has the best tanks money can buy. However,

at the tactical level, the threat drops to low because most of the tanks are in storage, have been cannibalized for parts, or are not being maintained well. At the operational level the threat rises to medium because this country has lots of tanks widely scattered, but drops down to low at the strategic level because the tanks simply cannot be sustained in battle long enough to be effective.

The results of this scrub confirmed in our minds one of the great dilemmas facing planners and the intelligence officers who support them:

- At the Service level, we need strategic generalizations in the planning stage and extremely precise technical specifics in the acquisition stage.
- At the theater level, we need operational generalizations for planning and tactical specifics for execution.
- Our training must take advantage of intelligence products at each level of analysis so that instructors at our basic, intermediate, and advanced schools can emphasize generalizations and specifics firmly related to our actual expeditionary environment and their

respective mission areas.

Each of these levels of analysis should be a completely different intelligence product. One should not have to wade through a 7-volume *Army Country Profile* or sign out 20 different intelligence products in order to arrive at these types of generalizations or specifics. The intelligence community, and especially the defense intelligence community, should be doing this, provided customers are prepared to define what generalizations and/or specifics they need.

For too long our individual Service components have defined our intelligence requirements in terms of essential elements of information (EEI) and statements of intelligence interest (SII), with the result that while we might receive copies of products containing material pertinent to those EEIs, we as a Service have had zero influence on what products are actually produced, what formats and media have been adopted, and what mixes of countries have been examined. SIIs are dissemination tools—they do not impact on production. It is intelligence produc-

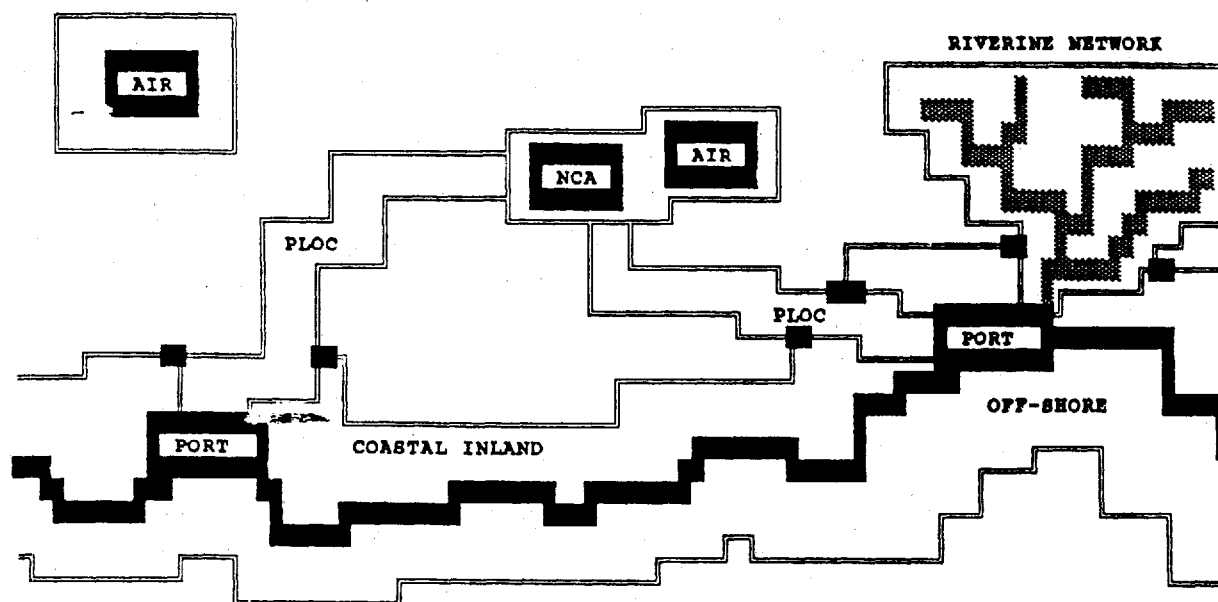
tion requirements (IPR) and the various commanders-in-chief (CinCs) needs that lead to specific products being created.

The single most valuable role the Marine Corps Intelligence Center can play in this regard is to start exercising some influence on all of the national and defense intelligence production facilities paid for with purple money and levying our specific production requirements on those organizations. I would hasten to add that such facilities have always been responsive and ready to cooperate—it is we who have failed in the past to define our needs in production terms. At the same time, it would be helpful if Marines understood that the Center is not intended to be an independent production facility, duplicating the efforts of others—rather it is intended to ensure, with a “bare bones” capability, that we get these other facilities to work for us and produce for ourselves only those essential tailored products that cannot be done by others.

In Table 7, a concept for an entirely new family of defense intelligence

STRATEGIC PRODUCT FAMILY		
C	P	(Mission Area, Regions, Timeframes)
OPERATIONAL PRODUCT FAMILY		
O	R	(For specific regions, generalizations by mission area and timeframe)
TACTICAL PRODUCT FAMILY		
T	I	(For each mission area, both generalizations and specifics by country, with emphasis on terrain & civil constraints)
TECHNICAL PRODUCT FAMILY		
Y	Z	(For mission areas, generalizations by region and timeframe, with specific details on sub-systems)
Mode of Delivery		
(Medium, Format, Classification)		

Table 7: Family of Defense Intelligence Products



OFF-SHORE: 25 NM TO HIGH-WATER MARK
COASTAL INLAND: HIGH-WATER MARK TO 50 K INLAND
PLOC: PRIMARY LINE OF COMMUNICATION FROM PORT TO NCA + 30 K EACH SIDE
NCA: NATIONAL CAPITAL AREA + NEAREST STRATEGIC AIR HEAD + 30 K ALL ROUND
INTERNAL: RIVERINE NETWORKS, OTHER STRATEGIC AIR HEADS OR CONCENTRATIONS OF PEOPLE, MILITARY, OR KEY INFRASTRUCTURE NODES

Table 8: Limiting the Area of Analysis

products that is responsive to specific customer groups at different levels of analysis is illustrated. Although the product families continue to provide for military order of battle information, this concept of intelligence production moves far beyond the "bombing encyclopedia" approach that has characterized much of defense intelligence's efforts in the past, and it brings us to the point where we can thoroughly integrate operational geography and civil factors of vital importance to combined arms and ground force operations.

As the accompanying tables suggest, military capabilities assessed in isolation from operational geography and pertinent civil factors can be seriously misrepresented. It is also important to note that planning and programming capabilities for the conduct of stability operations must be based upon on solid intelligence about nonmilitary factors that have traditionally been neglected by defense intelligence. We hope to make significant headway in this area over the next few years by working closely with Service planners and programmers to establish what they need in the way of products, and then working with individual elements of the

defense intelligence community to ensure we receive our "fair share" of defense intelligence production. We naturally need to ensure that this production addresses our mission-area factors in terms our operators define as pertinent, that it is provided at a level of classification and generalization acceptable to us, and that it is provided in a medium (e.g., electronic vice hard copy, with color graphics and manipulable spread sheets) that lends itself to follow-on exploitation. We are talking about nothing short of a radical change in the way defense intelligence does business.

Area of Analysis Limitation

Last, we learned that you cannot draw generalizations regarding topography and civil factors based on entire countries. This is true for military capabilities as well, if to a lesser extent. In coming to conclusions about cross-country mobility, for example, it made no sense to rule out a country that was two-thirds mountainous if most of the population and the military objectives were in a coastal plain. By the same token, if mobility between the beach and the capital city was restricted, and bridge loading conditions

restricted vehicle weight along main lines of communication to 20 tons, then we should be obliged to show the country as difficult even if large unoccupied areas are more favorable to ground mobility.

We subsequently developed Table 8, which illustrates those areas of interest that we are most concerned about and what areas of a specific country were considered in arriving at our generalizations.

If the intelligence community is unwilling to produce intelligence products of immediate value to individual customers with clear-cut requirements for both generalizations and highly technical specifics, then we have no alternative but to do it ourselves, using finished production from others and raw intelligence where necessary. More to the point, however, only Marines can truly understand their own environment and apply that intelligence to the training, equipping, and organizing of our Nation's finest force-in-readiness.

Marine Corps acquisition, known end to end as the concept-based requirements system (CBRS), has come a long way since the Marine Corps Combat Development Command and the Marine

Corps Research, Development and Acquisition Command (MCRDAC) were established. Still, there is more to be done. When Col Breede and I started the Marine Corps Intelligence Center, the first thing he asked me to do was interview key personnel, both in our Warfighting Center, where concepts and doctrine are developed and requirements are validated, and at MCRDAC. Subsequently, I supported congressional testimony by the Director of Intelligence on shortfalls in intelligence support to acquisition. Perhaps the most troubling shortfall mentioned was our intelligence community's failure to establish a family of products that was not classified, and our failure to establish convenient means for planners and program managers to request, receive, and exploit classified materials. I found that many of our most important planners and system acquisition managers wanted nothing to do with classified information—their offices were not cleared for what they wanted to hold; they tended to assume that once the required operational capability (ROC) document was approved, the "threat" ticket was punched; they didn't understand the intelligence community or how to make it work; no one had sponsored them for appropriate clearances; and they had no means of prioritizing their needs for ongoing threat support to their respective life cycles.

The following is a listing of five specific examples of intelligence failure in support of threat acquisition that I found to be common occurrences:

- Concept development that ignored threat and terrain generalizations, in some cases through reliance on outdated and implausible Marine Corps scenarios.
- Mission need statements (MNS) or ROCs that went "worst case" automatically without matching their requirements to the average threat likely to be found in a given area in terms of trafficability, hydrography, and weather. This was particularly the case when we were relying on Army or Navy system threat assessment reports (STARs), and there was no independent validation of these STARs against Marine Corps realities.
- MNSs or ROCs, including those that were joint, that did not address command, control, communications, and intelligence (C³I) support. It makes

no sense to build expensive, sophisticated platforms if they cannot receive the near-real time targeting intelligence they need to be effective during their very limited times on station.

- Numerous programs oblivious to the need for ongoing threat support. This is the only way these programs can remain viable and survive over the long-term. The fact that the acquisition process is usually so drawn out only exacerbates this problem.
- Finally, test and evaluation without foreign materiel support.

The former Commandant, Gen A. M. Gray, has noted in the past that the Marine Corps "cannot afford to train and equip for the wrong war." He has assured the President, Congress, and the American people that Marines will not only be the "first to fight," but also be able to "fight smart." Now that we have our own Intelligence Center designed to provide tailored threat support to acquisition, doctrine, and training commands that jobs should be a little easier. The Center also will provide support to the new Commandant, Gen Carl E. Mundy, Jr., as our Service chief and to the FMF when it cannot obtain the intelligence research and analysis it needs for contingency planning from other sources.

Now that we have come to grips with the fact that we cannot equip for every war, or even afford to equip for the wrong war, I hope all can agree that we must emphasize anew the importance of intelligence, on the one hand, and honest operational analysis on the other. We cannot be all things to all people. We have a rich history of constabulary and expeditionary operations, and we have a strong foundation as a self-sustaining, combined arms team with a naval character. If I could identify one area of weakness in defense intelligence overall and our Service in particular, it would be that of planning and programming in relation to real-world threats and terrain. The players are in place and we've experimented with the process, but now is the time to pay attention to what our intelligence professionals are telling us and plan accordingly. We need to focus in on the gray area between diplomatic chit-chat and sustained land warfare . . . everything in between is ours.



Caveat

The personal working paper which follows is just that--personal--and does not reflect the policy, perspective, or intent of any other individual or organization.

Further, while this working paper reflects an organized approach to the issue of how one might go about significantly increasing national intelligence support to American enterprise, and particularly clandestine human intelligence and national technical intelligence support, in fact it supports two conclusions:

- ◆ *First, that such additional classified efforts as may be undertaken should be restricted to "illuminating the playing field" for official U.S. government policy-makers. There is little return, and much risk, in attempting to provide classified information on a selective basis to any private sector individual or organization....and who is to say what constitutes a "national" or "American" enterprise?*
- ◆ *Second, that open sources represent a totally legal, politically safe, and rationally sound alternative to any increase in classified activities. It is particularly noteworthy, in an era of declining resources, that the return on investment (ROI) from open sources is at least an order of magnitude higher than that derived from the more traditional disciplines.*

I have an article in progress on this topic, and would welcome your insights. Please direct comments to steeler@well.sf.ca.us, or fax them to (703) 536-1776.

**NATIONAL INTELLIGENCE AND THE AMERICAN ENTERPRISE:
EXPLORING THE POSSIBILITIES**

Intelligence Policy Seminar Working Group #3
John F. Kennedy School of Government
Saturday, 14 December 1991

ISSUE: Should the U.S. government use its existing national intelligence resources and/or develop new "designs and methods" permitting the collection, analysis, and dissemination of intelligence intended to improve the economic competitiveness of the nation, larger industries, and specific American enterprises? If so, what should our national policy objectives, and what should be our national intelligence strategy be to achieve our objectives?

A. Subordinate Themes:

- (1) What are the policy implications?
- (2) What are the legal implications and requirements?
- (3) What are the President's priorities?
- (4) What are the resource implications?
- (5) What Congressional and/or political concerns exist?
- (6) What are implications for existing sources and methods?

B. Areas of Inquiry and Opportunity:

- (1) Illuminate the Playing Field
 - (a) Foreign Market Access (U.S. Overseas, Foreign Firms in U.S.)
 - (b) Government Support to Industry
 - (c) Government and Industry Strategy
 - (d) Trade Policy
 - (e) Monetary Policy
 - (f) Investment Regulation
 - (g) Product Standards (Legal Obstacles)
 - (h) Product Opportunities
 - (i) Costs of Production (Labor, Materials, etcetera)

- (j) Support to Negotiations
- (2) Level the Playing Field
 - (a) Background for Demarches
 - (b) Support to Legal Actions and Enforcement
 - (c) Background for Tariff Actions
 - (d) Market Limitations (Imports to U.S.)
 - (e) Remove Foreign Market Limitations
 - (f) Government Financial Support to Industry
 - (g) Exception to Anti-Trust for Joint R&D/Production
 - (h) Marketing Assistance
- (3) Tilt the Playing Field
 - (a) Acquire Foreign Trade Secrets
 - (b) Government Trade Financing
 - (c) Trade Policies
 - (d) Political/Military Leverage
 - (e) Product Development Financing
- C. Under What Circumstances?
 - (1) In all cases?
 - (2) In response and retaliation to similar activities by our competition?
 - (3) In only those areas where we are at an economic disadvantage?
 - (4) Where we have a deficit in our balance of trade or payments?
 - (5) In support of trade delegations and negotiations?
- D. Pertinent Peripheral Issues:
 - (1) Retraction of the Foreign Corrupt Practices Act?
 - (2) Sanctioning of American industrial espionage against

foreign competitors?

E. In What Areas of Endeavor?

- (1) Research & Development
- (2) Manufacturing Technology
- (3) Natural Resources
- (4) Foreign Weapons Competition
- (5) Banking & Monetary Policy?
- (6) Trade Policy?
- (7) Strategic Economic Directions and Opportunities

F. Assessing the Needed Infrastructure

- (1) What Are or Should Be the Mechanisms?
- (2) How Do We Level the Domestic Playing Field?
- (3) Could We Help Protect Our Secrets?
- (4) Would It Compromise Sources and Methods?
- (5) Do We Need New "Designs and Methods"?
 - (a) Collection Priorities and Capabilities
 - (b) Analysis Methodologies, e.g. "true cost of production" reflecting government assistance
 - (c) Multi-Media Database Construction
 - (d) Policy-Pertinent Presentation
 - (e) Accommodation of Legal Requirements for Testimony

G. Tentative Evaluation of Results

- (1) Would There Be a Positive Effect?
- (2) Would Industry Substitute Intelligence for Enterprise?
- (3) Would This Inhibit Competitiveness?

**NATIONAL INTELLIGENCE AND THE AMERICAN ENTERPRISE:
EXPLORING THE POSSIBILITIES**

Making It Happen

Areas of Interest: Areas of Action:	Customer(s)	Capabilities Today	Capabilities Needed
ILLUMINATE THE PLAYING FIELD	Government at policy/direct interest levels e.g. U.S. Trade Representative, Commerce, and Treasury	Relatively low in most areas, fair to good in a few areas of high policy interest	Although could be primarily a re- alignment of existing resources, would require a significant increase in dedicated manning and funding
LEVEL THE PLAYING FIELD	Expanded USG to include Justice, Customs, other enforcement activities	"War on Drugs" is model, has required adjustments in ways of doing business (classification and clearance differ- ences, evidence)	Would need new rules and methods to sup- port aggressive en- forcement actions without jeopardizing sources and methods.
TILT THE PLAYING FIELD	Expanded USG and some if not all private sector activities in some if not all areas of high interest	In neither the IC nor the enforcement and policy communi- ties are there the manpower structure, rules, or funding to take action	Increased ability of IC to provide actionable products would require match- ing increase in other executive agencies to effect change

Assessing The Ramifications

Areas of Interest: Areas of Action:	Professional Risk/Implications	Domestic Political Risk/Implications	Int'l Political Risk/Implications
ILLUMINATE THE PLAYING FIELD	Relatively low and subject only to policy leaks; would need to refine economic databases and methodologies	Could cause discom- fort to selected enterprises and affiliated politi- cians	Relatively low, generally would require increased collection efforts
LEVEL THE PLAYING FIELD	Increased risk to sources, risk of bad press and legal attacks; OSCINT higher ROI and reduced risk for impact	USG faces increased legal challenges and demarches from foreign government/ industry teams	Increased hostility to "imperial" U.S., likely propaganda from Third World as well as more subtle and powerful EEC
TILT THE PLAYING FIELD	Potential divi- sive fracturing of community-- must develop new methods for both collection and protection	Increase of risk	Increase of risk

Estimating the Resource Requirements

Areas of Interest: Areas of Action:	Collection	Analysis	Dissemination
ILLUMINATE THE PLAYING FIELD	Much more HUMINT as well as tactical SIGINT	New methods, more people	Begin to develop means of protecting sources
LEVEL THE PLAYING FIELD	Redirection of national assets, focus on priority areas (need to change priorities in all guidance documents)	Significant investment needed in OSCINT data entry including "gray" publications; new databases, methods	Radical change in product lines, and in rules of evidence and/or standards for policy exploitation
TILT THE PLAYING FIELD	Radical increase and change in nature of assets employed overseas with change in rules regarding domestic collection.	May need to have analysts in direct support of both USG enforcement and selected U.S. enterprises	Need entirely new structure for C4I2, along lines of existing paths and processes for war on drugs but extended to select private entities.

UNITED STATES MARINE CORPS
COMMENTS ON
JOINT OPEN SOURCE TASK FORCE REPORT AND RECOMMENDATIONS
(WORKING GROUP DRAFT DATED 6 JANUARY 1992)

Prepared by Robert D. Steele
C4I2 Department, Resource Staff
(703) 693-5422

11 January 1992

FINAL REPORT--PROVIDED FOR INFORMATION

Contents

Executive Summary.....	1
Introduction.....	2
Summary of Report Deficiencies.....	4
Summary of Marine Corps Views.....	6
Detailed Critique of the Report.....	11
Military View of OSCINT.....	21
Military Consumer's Viewpoint.....	24
Military Producer's Viewpoint.....	32
Military Collector's Viewpoint.....	34
Survey of Existing Capabilities: Military Views.....	37
Military Wargame Results.....	38
Survey of Unfulfilled Military OSCINT Requirements.....	43
Conclusion.....	44
Bibliography.....	45
OSCINT Points of Contact.....	48
Glossary.....	50

EXECUTIVE SUMMARY

The report as drafted fails to satisfy the guidance provided by the Director of Central Intelligence...

There are two major problems with the report:

(1) It has not been properly staffed--this is not to cast blame, only to point out that the combination of a very short timeframe and disconnects within and outside the Task Force have resulted in an extraordinarily limited document which fails to provide the Director of Central Intelligence (DCI) with the necessary balanced view of national open source intelligence (OSCINT) requirements and capabilities as well as an estimate of the resources necessary to fulfill those requirements by developing the needed capabilities.

(2) The report fails to integrate the perspectives of a very broad community of military, non-military, and private sector consumers, and lacks vision in other areas--no document which fails to recognize the severe deficiencies in our existing capabilities, much less the radical shortfalls in meeting emerging requirements, can be considered satisfactory.

Over-all the approach taken by the Task Force is one of incremental adjustment designed to limit requirements, rather than one of radical realignment designed to satisfy requirements.

The report fails to meet the essential requirement for Executive action and Congressional support: it does not define the problem, the desired outcome, or the means by which a national OSCINT strategy and capability can be established for the benefit of the government as well as the private sector.

We recommend that an entirely new Task Force be constituted, under the leadership of the Administrator of the Defense Technical Information Service (DTIC), and with the assistance of elements of the intelligence community. This is one instance when the intelligence community does not have the internal expertise to fully define the requirements and the needed capabilities. A complete report, to include detailed manning, funding, and facilities requirements, as well as program objectives and milestones, can be ready within ninety days of commission.

INTRODUCTION

...we believe that our concerns and our recommended improvements are generic in nature and would be endorsed by the broad majority of OSCINT collectors, producers, and consumers--inside and outside the intelligence community--that were not consulted in the preparation of this report to the DCI.

This report complements the Task Force report in that it does not disagree in principle with any of the Task Force recommendations. However, the Task Force report reflects a limited understanding of the widespread demand for OSCINT in the military--and by extension in other areas of the government--and fails to offer innovative and long-range prescriptions for improving our Nation's capability in this area.

This report amplifies the Task Force report--to the extent possible under the established deadline of 15 January 1992--by proposing three specific initiatives, one a "quick fix" for FY 92, the others a comprehensive combination of a \$50 million/40 person initiative for FY 93-97, and a \$100 million/80 person initiative for FY 94-99--together these initiatives establish a national capability for OSCINT collection, computation, and communication--a capability which will meet the needs of users throughout the government and in the private sector.

Finally, this report diverges from the Task Force report in that we believe the OSCINT situation within the existing Intelligence Community is indeed in disarray; that the Task Force has failed to solicit a full range of consumer and producer commentary on requirements and capabilities; and that the Task Force report is in error when it states that its conclusions reflect the consensus of the Intelligence Community.

The most basic problem with the Task Force report is that it has provided a relatively good definition of open sources, albeit failing to include multi-spectral imagery (MSI), and then proceeded to ignore the vast shortfalls in global collection, processing, and exploitation of these same sources.

The final draft states:¹

¹ Open Source Task Force, "Joint Open Source Task Force Report and Recommendations" (Working Group Draft dated 6 January 1992, S), page 2.

"By Open Source we refer to publicly available information appearing in print or electronic form. Open Source information may be transmitted through radio, television, and newspapers, or it may be distributed by commercial databases, electronic mail networks, or portable electronic media such as CD-ROM's. It may be disseminated to a broad public, as are the mass media, or to a more select audience, such as gray literature, which includings conference proceedings, company shareholder reports, and local telephone directories. Whatever form it takes, Open Source involves no information that is classified at its origin; is subject to proprietary constraints (other than copyright); is the product of sensitive contacts with U.S. or foreign persons; or is acquired through clandestine or covert means.

The report fails to come to grips with the complexity of the open source world and the means required to collect, compute, and communicate OSCINT across all topical areas and all political and cultural boundaries. The report fails to reflect either the obstacles or the opportunities in terms of sources, producers and production media, and consumers with mutual interests (not only within the government as a whole, but including the private sector and ultimately foreign organizations).

This Marine Corps report will first discuss in detail our concerns with the draft report proposed for submission to the DCI, and will then provide substantive information about our view of needed improvements in the over-all national OSCINT situation. While our views must of necessity focus on what we have learned as a military service, and reflect our experience in standing up a new National Foreign Intelligence Program (NFIP) analysis and production facility (the USMC Intelligence Center), we believe that our concerns and our recommended improvements are generic in nature and would be endorsed by the broad majority of OSCINT collectors, producers, and consumers--inside and outside the intelligence community--that were not consulted in the preparation of this report to the DCI.

SUMMARY OF REPORT DEFICIENCIES

We do not see a balanced approach to OSCINT in the draft report.

The report does not reflect the scope and depth of open source requirements from the broad intelligence, defense, and non-defense communities.

The report as drafted fails to satisfy the guidance provided by the DCI in three substantial ways:

(1) The report does not address the DCI's interest in examining ways in which the proliferation of open source materials of all kinds (emphasis added) can be handled. The Marine Corps has a very strong interest in commercial MSI and considers OSCINT to be an all-source discipline. The report reflects a lack of familiarity with OSCINT developments throughout the broader community and the private sector, a probable result of early domination of the draft by individuals most familiar with text processing to the exclusion of commercial database exploitation, foreign video broadcast exploitation, defense attache reporting and domestic collection, LANDSAT/SPOT exploitation, and related commercial-off-the-shelf (COTS) applications and industrial internal research & development (IR&D) efforts. We do not see a balanced approach to OSCINT in the draft report.

(2) The report does not reflect the scope and depth of open source requirements from the broad intelligence, defense, and non-defense communities. As a result, the report seriously understates the deficiencies in our all-source OSCINT requirements and related capabilities.

(3) The report does not reflect the experience, views, and recommendations of most community OSCINT experts, nor does the report reflect the experience, views, and recommendations of those in the private sector who have spent significant resources on these issues. A number of individuals recognized for their contributions to OSCINT over the years, many of them senior Central Intelligence Agency employees, have not had an opportunity to contribute to the report.

The report specifically fails to address or enumerate the needs of the Services, the theater Commanders-in-Chief (CINC), or the defense intelligence functional managers, and it does not address requirements and capabilities needed outside the

intelligence community but directly pertinent to the ability of the community to fulfill competing requirements for classified collection, processing, and production.

The report fails to identify unfunded deficiencies of other elements of the government which have a specific role to play in the OSCINT arena--the Federal Research Division (FRD) of the Library of Congress (LC), for instance, has been unable to respond to seventy per cent of the requirements identified to it over the past several years, for lack of funding. No one in FRD was consulted by the task force members.

The report fails to describe the manning, dollars, facilities, and capabilities that exist today, and fails to provide any specific idea of manning, dollars, facilities, and capabilities that are required in the future.

The report fails to identify the major role which must be played by the private sector if our national OSCINT requirements are to be met. The privatization of encyclopedic data, to include geographic information, must be dramatically accelerated.

The report identifies the copyright issue but fails to examine the urgent requirements for modernization of the legal framework governing open sources.

The report fails to address counterintelligence and competitive activity needs in relation to our national open sources.

The report is over-classified and of limited utility as a basis for further investigation into OSCINT requirements and needed capabilities which are the focus of the DCI's inquiry.

SUMMARY OF MARINE CORPS VIEWS

Our greatest shortfall in OSCINT is our lack of definition of the requirements, and particularly the degree to which OSCINT products can be substituted for classified products.

Our greatest shortfall in OSCINT is our lack of definition of the requirements, and particularly the degree to which OSCINT products can be substituted for classified products.²

(1) Community surveys have concentrated on identification and description of existing open source databases and services;

(2) Industry, notably The MITRE Corporation, has done well at defining how technology can be applied to open source information;

(3) No one has attempted or adequately defined what consumers throughout government (much less throughout the private sector) require in terms of OSCINT, nor how OSCINT could be substituted for more expensive fragmentary compendiums of classified information.

We must distinguish OSCINT from clandestine or overt human intelligence (HUMINT) as a means of focusing executive attention on foreign print and voice/video media whose timely exploitation is critical to our national competitiveness, and to ensure the inclusion of MSI and other commercial imagery capabilities.

(1) OSCINT offers highest return on investment of any discipline/source area;

² The Marine Corps and its leadership have been actively pursuing open source solutions to intelligence information deficiencies for over two years. The establishment of the USMC Intelligence Center at Quantico in November 1987, and intensive efforts by the Center to obtain Third World information unavailable from classified databases, led to the development of an "Open Source Exploitation Strategy", a joint effort between the Marine Corps Combat Development Command (MCCDC) and the USMC Intelligence Center. For a description of the strategy see K. Muzbeck and M.B. Garnot, "Establishment of Electronic Open Source Exploitation Capabilities for Quantico Community; Enhancements to Existing Breckenridge Library Funded by Intelligence", Memorandum dated 4 April 1989.

(2) OSCINT has no advocate and there is no structure through which competing and duplicative initiatives can be integrated;

(3) OSCINT is cross-disciplinary (includes signals and images) and shouldn't be strictly a HUMINT endeavor;

(4) We need to scrub our requirements, both current and future, to determine shortfalls in capabilities for obtaining OSCINT (technical journals needing digitization, needed attaches and data entry coordinators by topical area and region, and government subsidization or long-term contracting for MSI production.

(5) Existing priority documents can be used to guide OSCINT--it is the resource managers who have been neglecting OSCINT's potential.

We should establish an OPEN SOURCE COMMITTEE with a mix of consumer, production, collection, ADP, budget, and R&D representatives...

We should establish an OPEN SOURCE COMMITTEE with a mix of consumer, production, collection, ADP, budget, and R&D representatives; task them with consolidating FY 92-97 resources and establishing a spending plan for government side of concept:

(1) Immediate objective in FY 92 should be establishment of an OPEN SOURCE COMMITTEE with a Chairperson (Senior Intelligence Service), Executive Secretary, Research Assistant, and Secretary --we should consider the possibility of establishing the committee at the Senior Inter-Agency Group level rather than at the Intelligence Community Staff (ICS) level in order to fully integrate all elements of the government;

...establishment of a national joint government-private sector Center for the Exploitation of Open Sources (CEOS).

(2) FY 92-97 target should be \$50 million and 40 people to establish a national cooperative Center for the Exploitation of Open Sources (CEOS) to serve as a central repository and satisfy minimal mandatory requirements for open source research such as is normally conducted by the FRD. Both funds and manning could to be found within existing initiatives in President's Budget and

proposed to SSCI/HPSCI for consolidation;

(3) FY 94-99 target could be additional \$100 million and 80 people responsible for coordinating global academic and business data entry responsibilities by topical and regional area, perhaps through a National Knowledge Foundation (NKF) or National Science Foundation (NSF) process. For both of the latter initiatives:

(a) New Naval Intelligence Center (NIC) building at Suitland may have space due to cut of 500 people from its projected occupancy--approximately 75,000 square feet, some since allocated to other requirements, was freed up by the cut in manning;³

(b) Alternative site, not available until FY 95 if at all, is old Foreign Science & Technology Center (FSTC) building --this site is particularly attractive if FSTC does obtain the new building because the old building complex lends itself to a government site in what was the Sensitive Compartmented Information Facility (SCIF), and rental of the various floors in the main building to private sector partners. The proximity of the University of Virginia, the rural but accessible location, and the likely support of the senior Senator from Virginia make this the most attractive alternative;

(c) A West Virginia location may also be worth considering due to interest of the Chairman of the Senate Appropriations Committee.

We should designate a focal point or executive agent for OSCINT exploitation. An expansion of the Defense Gateway Information System (DGIS) and integration of CEOS into the DTIC structure, or a cooperative venture between DTIC, the National Technical Information Service (NTIS), and FRD would be good starting points.

(1) Government sponsorship of a central repository to which both government and private users can gain access will permit control and security auditing as well as optimize government exploitation;

(2) Government sponsorship, through broad dissemination of the functional requirements concept and related system specifications of the Computer Aided Tools for the Analysis of Science and Technology (CATALYST), will help establish a generic

³ NIC already is programmed to receive one important OSCINT capability. For a description see Information Handling Committee, "Establishment of the Centers for Ocean Surveillance and Maritime Information Coordination (COSMIC)", Draft Concept Paper, Fax dated 15 March 1991.

analysis "toolbox" as useful to business and academia as to government;

We need to understand, through a comprehensive survey as well as ongoing auditing, how our national open source databases are being exploited and what the threat is to proprietary financial and technical information.

(3) We need to understand, through a comprehensive survey as well as ongoing auditing, how our national open source databases are being exploited and what the threat is to proprietary financial and technical information;

(a) We can help private enterprise protect what it must protect to remain competitive in research and development;

(b) While we cannot and should not try to restrict access to public databases, knowing how these databases are being exploited by others could help justify our own program of foreign open source exploitation to Congress

(c) A Special National Intelligence Estimate (SNIE) should be requested and completed immediately.

Possibly under Department of Commerce leadership, we should seek establishment of a joint government-business "Blue Ribbon" Commission, ideally chartered by the President, to rapidly outline objectives, milestones, and a spending plan for the private (business and academic) side of the OSCINT concept...

Possibly under Department of Commerce leadership, we should seek establishment of a joint government-business "Blue Ribbon" Commission, ideally chartered by the President, to rapidly outline objectives, milestones, and a spending plan for the private (business and academic) side of the OSCINT concept:

(1) Privatization of data entry--corporate adoption of individual countries, scientific and technical areas, or specific recurring publications is essential--government cannot afford to unilaterally build and maintain a global data entry infrastructure;

(2) Creation of selected academic focal points, nurtured and guided by a NKF/NSF process in monitoring open source data in

particular topical and regional areas, will provide both government and the private sector with sources of expertise, and stimulate greater coverage; and

(3) Recognition that our cooperative (but government-controlled) repository will be but one of many; the broader concept of "national knowledge management" must begin to emerge, and be built upon an infrastructure which links all automated databases and gradually develops a national knowledge collection and processing plan which encompasses all information, not just information of "intelligence" value.⁴

⁴ It is imperative that the intelligence community efforts to improve OSCINT not only be coordinated with others in and out of government who have mutual interests, but that our OSCINT effort be fully integrated with major computing and technical initiatives such as those of the Federal Coordinating Council for Science, Engineering, and Technology ("Grand Challenges: High Performance Computing and Communications"), related "computer superhighway" concepts coming off the Hill, and the forthcoming Presidential "National Technology Initiative" being crafted by the Departments of Commerce and Energy. For a description of the latter initiative's genesis, and its plan to reorganize the nation's 726 laboratories to gain the best return on federal investment, see Lucy Reilly, "Bush Shift Adds Tech to Agenda: Cabinet, Industry to Craft National Policy", in Washington Technology (9 January 1992), page 1. We must establish a national knowledge management strategy and a bridge to a national information technology architecture. OSCINT must be part of the fabric of the nation, not an isolated esoteric discipline.

DETAILED CRITIQUE OF THE REPORT

The report's attempt to dispel the impression that OSCINT is in disarray reflects a parochial view that is inconsistent with the rapidly changing information situation and the rapidly changing needs of military and non-military consumers in government, as well as consumers in the private sector.

Page 1

The report focuses on the Foreign Broadcast Information Service (FBIS)--and later in the report on the Office of Information Resources (OIR) and the Foreign Aerospace Science & Technology Center (FASTC)--to the exclusion of such other organizations as FRD, NTIS and DTIC/DGIS. Throughout the report the emphasis is on the traditional producers of the limited types of OSCINT familiar to the community, and not--as should be the case--on the consumers.

The drafters of the report are focusing on collection and processing redundancy when the greatest problem is the lack of a global data entry capability spanning the full range of media (text, interview, voice broadcast, video broadcast, and commercial imagery including MSI).

The report exaggerates the "inherent versatility, responsiveness, and sectoral expertise of the existing Open Source sector".

Page 2

The report alludes to the importance of OSCINT as a means of reducing the demands on other collection disciplines. This is important, but needs to be stressed, with emphasis being placed on the gross imbalance between expenditures on the other disciplines versus expenditures on OSCINT.

"Only when easy, open sources prove insufficient, or clearly require cross-checking--and national technical means require augmentation--should American intelligence management begin to think about other collection efforts."⁵

⁵ George A. Carver, Jr., "Intelligence in the Age of Glasnost", Foreign Affairs (Summer 1990), page 158.

"American intelligence analysts now have to cope with a torrent of information and data. Amid an exponential proliferation of satellites and fiber optics, interlinked computers and data bases, modems and FAX machines, 24-hour cable news, and the opening of area, subjects, and all manner of sources that until recently were shielded, proscribed, or denied, these analysts are becoming information junkies, never far from an overdose. If effectively harnessed and channeled, then astutely exploited, this new information and data flood can dramatically improve the quality and accuracy of American intelligence assessments and estimates on all manner of crucially important subjects; but it creates new complexities as fast as it clarifies old mysteries. In a flood, furthermore, it is easy to be overwhelmed and drowned if one is not both sensible and careful." (emphasis added).⁶

The report's attempt to dispel the impression that OSCINT is in disarray reflects a parochial view that is inconsistent with the rapidly changing information situation and the rapidly changing needs of military and non-military consumers in government, as well as consumers in the private sector. The report reflects no understanding of who the "end users" are, nor the distinctions between their needs.⁷

The report severely understates the global data entry problem and the need for both a massive collection and digitization effort conducted by the private sector with government assistance and direction, and an international pattern of information exchange agreements in which foreign information is acquired in digital form.

Page 3

The report reflects a lack of understanding of the utility and scope of the U.S. Foreign Intelligence Requirements Categories and Priorities (FIRCAP) maintained by the Foreign Intelligence Priorities Committee (FIPC).

⁶ Ibid., page 159.

⁷ What is remarkable about this conclusion on the part of the Task Force is that it flies in the face of all published evidence, including the findings of the House Appropriations Committee (HAC) investigation, "Exploitation of Unclassified Media for Intelligence Purposes" (15 March 1989). Highlights from this report are contained in George L. Marling, "HAC Staff Report on Open Source Exploitation" (Memorandum for the Record dated 6 November 1989, S).

The report is correct in highlighting the critical and obstructive nature of copyright and contract limitations on the exploitation and dissemination of open source materials, but misses the point: in the era of electronic information, it is the law which must change, not the medium and its use. So-called "hackers" are in fact information entrepreneurs, the "robber-barons" of the new frontier--the prophets of the age of cyberspace. The Intelligence Community must help policy-makers and the public understand the need for a new legal framework in which restrictions on the utilization of information, information as the new "Commonweal", are not tolerated.⁸

The report is seriously misleading when it states that "pulsing" and related surveys conducted for the report "not only validated the views and conclusions of previous studies but significantly, surfaced an encouraging spirit of cooperation among Open Source organizations". There are three problems with this view:

(1) The previous community reports are of marginal utility in assessing OSCINT requirements. The best of the reports, under the auspices of the Intelligence Producers Council (IPC) and the HUMINT Committee, both with the assistance of the Information Handling Committee (IHC), ably documented existing OSCINT data bases and areas of endeavor throughout the community.⁹ The report of the Strategic Planning Working Group has not been

⁸ This in no way ignores the rights of information producers to royalty fees and other remuneration; in the same way that technical means must be developed to seal, authenticate, and validate raw information, such means must be extended to track the accession, extraction, integration, and transmission of raw information such that the originator is recognized and rewarded in an appropriate manner. What cannot be tolerated or condoned by law is any restriction on the private or public exploitation of open sources. There are remarkable analogies between the archaic law of information and the laws of discrimination which previously sanctioned severe constraints on the liberties of people of color.

⁹ Cf. Intelligence Producers Council, Report on Automated Open-Source Data Bases (Draft August 1990, final due out April 1991, S/NF/NC); HUMINT Committee, Directory: Information Resources Based on Foreign Media and Publications (DCIC 10006-85, HC 85-207, July 1985, FOUO); and HUMINT Committee, Directory: Information Resources Based on Foreign Media and Publications, Annex (DCIC 10007-85, HC 85-208, July 1985, S/NF). Another report which has been cited by others but not widely circulated is the Open Source Exploitation Program (March 1986), approved by then Acting DCI John McMahon.

widely disseminated, and is viewed by many of those who have seen it as being relatively useless. Not one of these reports has adequately distinguished between the varying consumer groups and the different sources of OSCINT, nor established with any credibility or specificity the requirements and the capabilities needed to satisfy those requirements.¹⁰

(2) The report does not reflect the views of the broader community and a wide variety of experts familiar with OSCINT. Among those who were not consulted in a timely or thorough fashion:

(a) Service Chiefs and their staffs

(b) Theater Commanders-in-Chief

(c) Defense Intelligence functional managers

(d) Assistant Secretaries of Defense (notably for Special Operations/Low Intensity Conflict, where OSCINT is especially important)

(e) FRD/LC, where 70% of the studies requested by elements of the government over the past three years could not be carried out for lack of funding;¹¹

(f) Most defense intelligence production facilities;

(g) Most Federal Contract Research Facilities (FCRF), including The MITRE Corporation which has been investing 10 man years and half a million dollars each year in OSCINT technology applications and requirements;¹² and

¹⁰ By contrast, the HAC report, supra note 7, as cited in Mr. Marling's memorandum, notes in detail the problems facing the community, including the fact that users of open source information are dispersed, are often remote from and unknown to the collectors or producers of the open source information, and do not have a financial stake in what is collected and processed.

¹¹ Personal discussion with Dr. Louis R. Mortimer, Acting Chief, Federal Research Division, 8 January 1992, Headquarters U.S. Marine Corps. Dr. Mortimer's staff has kept detailed records of requested studies and cost projections.

¹² For a useful review of what constitutes a minimal mandatory OSCINT research capability for a hypothetical organization, and a review of the internal research & development initiative sponsored by The MITRE Corporation, see Open Source Processing Research Initiative (OSPRI), Draft MITRE Technical Report, 6 January 1992.

(h) Many of the relatively few OSCINT experts available within the government and the private sector.¹³

(3) Because the report does not reflect the broader view, it exaggerates the utility and reach of the efforts it does recognized (e.g. the excellent work by the Intelligence Community Librarians Committee) while failing to understand the severe deficiencies in areas beyond its ken (e.g. the desperate military and humanitarian needs for LANDSAT and SPOT imagery).

Page 6

The report confirms its inadequacies in recognizing only two kinds of users: analysts, and members of the science & technology community. As will be documented in the section on military requirements, there are a wide variety of military OSCINT users at the strategic, operational, tactical, and technical levels--there are undoubtedly equivalent communities of users in the commercial and academic sectors, and in other parts of the government, that the report fails to identify.¹⁴

Page 7

The statement that "(m)uch of the basic architecture to address (the OSCINT) challenge exists..." is misleading if not false. There are insurmountable obstacles to the integration of OSCINT into most intelligence processing systems, obstacles that will not be addressed until the community comes to grips with the need for a data-driven architecture that is seamless and affords analysts transparent access to multi-media multi-lingual data at multiple levels of security.¹⁵

¹³ The most well-known, and interested Executive and Congressional staff, are listed in the final section. Others could be identified for specific areas of interest by those listed.

¹⁴ For an overview of the military requirements which OSCINT can satisfy, and a distinction between the users at the four levels of need (strategic, operational, tactical, and technical), see Robert D. Steele, "Intelligence Support for Expeditionary Planners", Marine Corps Gazette (September 1991), pages 73-79.

¹⁵ The report does not recognize the inherent limitations of the existing intelligence community organization, and does not put forth any innovative ideas for creating new capabilities. For one view of how the community should be approaching change, see Keith Hall, "Challenges Faced by U.S. Intelligence", American Intelligence Journal (Summer/Fall 1990), pages 1-3.

The Department of Defense, including as primary elements the DTIC and the Joint National Intelligence Development Staff (JNIDS), would be an excellent candidate for the role of Executive Agent...

The report is correct in identifying the need for an Executive Agent. The Department of Defense, including as primary elements DTIC and the Joint National Intelligence Development Staff (JNIDS), would be an excellent candidate for the role of Executive Agent, with the special advantage of having at hand military intelligence personnel able to "jump start" the data collection and digitization effort in peacetime.

The report's reference to "common concern" archives is misrepresentative in that most of these archives pertain to traditional denied area targets and are of limited value to the wide variety of customers concerned with the Third World and emerging threats that are non-governmental, non-conventional, non-linear in development, random in occurrence, and unfettered by rules of engagement (ROE) or doctrine.¹⁶

Page 8

The report's assumption that "technologies are not yet sufficiently mature to settle on standards or to undertake immediate large scale system integration" is of questionable validity. Not only are there a number of COTS applications and capabilities that are integratable under an open systems architecture in conformance with those international standards that are established, but now, at a time when the OSCINT media and data flows are changing in radical ways, is exactly the time to begin a global international effort to agree on data standards and other protocols which will facilitate data exploitation regardless of changes in technology.

¹⁶ For a clear distinction between the conventional and the emerging threat, see General Alfred M. Gray, "Global Intelligence Challenges in the 1990's", American Intelligence Journal (Winter 1989-1990), pp. 3-7, esp. p. 5. For additional commentary on why the existing intelligence structure is unable to deal with emerging issues, see Robert D. Steele, "Intelligence in the 1990's: Recasting National Security in a Changing World", American Intelligence Journal (Summer/Fall 1990), pp. 29-36, esp. p. 30-33.

Page 10

While the report recognizes the need for a clearinghouse mechanism and the value of end-to-end prototyping, it does not highlight the existing success stories, including CATALYST as developed by the Office of Scientific & Weapons Research (OSWR); the role of JNIDS in helping import and export such applications; the role of the Intelligence Research & Development Council (IRDC) Advanced Information Processing and Analysis (AIPA) Steering Group, and the fact that the single biggest obstacle to developing integrated OSCINT and classified analysis toolkits is the fragmentation of both the research & development (R&D) and the Automated Data Processing (ADP) communities within individual agencies as well as the community at large.¹⁷ A new Deputy Director for R&D and a new Deputy Director for Communications and Computing, each with budget authority across organizational lines, should be considered.

Page 11

The report's focus on FBIS, OIR, and FASTC is evident, and reflects an incredibly narrow view of OSCINT which fails to address the concerns and interests of the DCI, the President, or Congress.

The report exaggerates the value of FBIS reporting, which often serves as no more than a record of current media reporting.

The report properly recognizes the absence of a dedicated collection infrastructure, but fails to recognize both the magnitude of the multi-media collection problem, and the need for a cooperative government-private sector endeavor which is ultimately international in nature.

¹⁷ It merits comment that the finest example of a working prototype for an analyst's toolkit, one which relies heavily on open source input, was developed by analysts and not by ADP "professionals". CATALYST should be stabilized and exported throughout the community as quickly as possible. A complete report on generic functional requirements addressed by CATALYST is provided in Diane Q. Webb, CATALYST: A Concept for an Integrated Computing Environment for Analysis (CIA/DI/OSWR, October 1989). A complete report on the operational prototype now used by over forty analysts is provided in Samuel Hahn and Don Parrish, CATALYST: Sketching the Steps Toward an Integrated Computing Environment for Analysis (CIA/DI/OSWR, October 1991). The latter document identifies a number of funded and unfunded development areas.

In focusing on non-traditional sources, the report ignores the single most important open source for military operations, that of multi-spectral imagery and commercial overhead photography.

Page 12

In focusing on non-traditional sources, the report ignores the single most important open source for military operations, that of multi-spectral imagery and commercial overhead photography.

The report erroneously suggests that the existing "infrastructural complex represented by these three common concern organizations is capable of providing broad access to commercial data bases and gray literature...given adequate resources." These organizations are not structured, nor culturally suited, to meet the much broader and comprehensive demands of the wide variety of users whose needs are not addressed by the report.

The report as a whole...fail(s) to provide specific recommendations for needed manpower, funding, facilities, and capabilities.

Page 13

The report as a whole, and this section in particular, fail to provide specific recommendations for needed manpower, funding, facilities, and capabilities.

Page 14

The report's statement that "there is general accord among Open Source producers and users" is grossly misleading.

The report's focus on the Country Team as the source of most foreign publications and gray literature reflects a significant lack of appreciation for the capabilities of the military and the private sector.

Page 15

The report, in focusing on the need to understand what is stored and where, fails to recognize that the greatest problem facing the community is that of global collection and data entry--a central digitization facility and gateway (the latter recognized by the report as a requirement), which provides on-line access to all databases throughout the community, is an essential element of the OSCINT solution.¹⁸

Page 16

OSCINT is multi-disciplinary, and the HUMINT community, devoted as it is to the clandestine arts, is unsuited to manage the community effort. A separate OSCINT Committee, as recommended by the former Commandant of the Marine Corps, is required.¹⁹

The report's most disturbing failure of vision is reflected in its abject acceptance of the possibility that the Department of Justice will support existing copyright and royalty conventions, and not help develop an entirely new legal frame of reference for information handling, a frame of reference consistent with the President's desire to increase our national competitiveness.

Page 17

The report's most disturbing failure of vision is reflected in its abject acceptance of the possibility that the Department of Justice will support existing copyright and royalty conventions, and not help develop an entirely new legal frame of reference for information handling, a frame of reference consistent with the President's desire to increase our national competitiveness. Information needs to be treated--if necessary --as an eminent domain issue, but should ideally be established

18 For a concise detailed commentary on the necessary national knowledge management strategy, and specific recommended changes within the intelligence community to accommodate our OSCINT requirements, see Robert D. Steele, "Applying the New Paradigm: How to Avoid Strategic Intelligence Failures in the Future", American Intelligence Journal (Autumn 1991), pages 43-46.

¹⁹ Supra note 16.

as part of the "commonwealth", with provision for the recognition and reward of the information originators (no longer "owners"). We must pursue and expand the concept of "fair use" by developing electronic measures which allow new legal concepts to be enacted.

Page 19

In considering the array of alternatives the report fails to describe a CEOS-like capability, a concept articulated in a number of cited references and originally conceived of by the IHC staff as an Open Source Information Exchange (OSIX), but rather settles for the concept of a center which appears to be no more than a coordinating mechanism. Throughout the report one

(The report authors) appear to believe that the mechanisms they describe will help prioritize requirements so they can meet the most important ones in an orderly fashion. This concept is 180 degrees off the mark and amounts to limiting the Nation's OSCINT capability...

...what we really need is a "paradigm shift", a 100X to 1000X increase in resources devoted to OSCINT, and an approach which seeks to identify and fully satisfy ALL requirements for open source exploitation

receives the impression that the authors think the existing structure is sound and needs only an incremental increase in resources. They appear to believe that the mechanisms they describe will help prioritize requirements so they can meet the most important ones in an orderly fashion. This concept is 180 degrees off the mark and amounts to limiting the Nation's OSCINT capability--those of us who have been actively involved in establishing OSCINT requirements understand that what we really need is a "paradigm shift", a 100X to 1000X increase in resources devoted to OSCINT, and an approach which seeks to identify and fully satisfy ALL requirements for open source exploitation. The report also does not consider the possibility and desirability of a NKF/NSF effort to nurture and guide efforts in the private sector.

MILITARY VIEW OF OSCINT

...persistent deficiencies in how the United States Government (USG) as a whole collects, computes, and communicates open source information and OSCINT.

The report commissioned by the DCI could reasonably be expected to break new ground in the area of OSCINT. Unfortunately, for reasons associated with both a lack of time and bureaucratic myopia, the report as drafted does not offer any significant contribution to the resolution of the OSCINT challenge. Below we provide a military perspective on OSCINT requirements and needed capabilities.

Building upon our understanding of the overwhelming demands from a wide variety of consumers of intelligence, both in and out of government, this material postulates a number of persistent deficiencies in how the United States Government (USG) as a whole collects, computes, and communicates open source information and OSCINT. This is not to say that the existing capabilities for exploiting OSCINT are "broken"--they are simply inadequate to the meeting vastly increased needs for OSCINT by the government as well as the private sector, including not only U.S. firms but also the academic community and the individual American citizen. Further, if one scrutinizes the charters of these organizations, there are grounds for suggesting that they are not fulfilling their mission, and that their charters and their budgets require revision.

The President has clearly stated his desire to improve our competitiveness as a Nation. While there has been much discussion about the relative merits of using national intelligence to support American enterprise, such a course is fraught with difficult questions of legality and fairness. A far better approach--one which is both relatively inexpensive and provides a greater return on investment than is common to the traditional intelligence disciplines--is to focus on improving our Nation's access to open source information, from which each consumer can derive tailored OSCINT.

Within the government, the era of confrontation and containment, an era which required vast expenditures of funds to maintain a sophisticated and continuous technical watch over "denied areas", is decisively ended. There are still requirements for covert technical capabilities and their human counterpart--clandestine operations--but these must be refined and in some cases radically altered to enable them to be

effective against emerging threats which are not as readily identifiable as the nuclear and conventional forces of a very few

In an era of radically declining resources, it is imperative that our covert and clandestine capabilities be focused on those priority topics and areas for which there is no OSCINT alternative. OSCINT should be our first line of analysis.

governments. In an era of radically declining resources, it is imperative that our covert and clandestine capabilities be focused on those priority topics and areas for which there is no OSCINT alternative. OSCINT should be our first line of analysis.²⁰

The threats of the future, including environmental deterioration and natural catastrophe, technological proliferation as well as unanticipated and complex break-down, demographic rampages, etcetera--and the opportunities of the future, including strategic transnational economic alliances and information sharing--all require a return to scholarship.

Such scholarship is complicated by the vast out-pouring of multi-media multi-lingual information from every corner of the globe. Our concepts and organization have simply not kept pace with the changing realities of information access and information technology. We have failed to develop a national knowledge management strategy and a commensurate national information technology strategy.

²⁰ It would not seem necessary to emphasize or document this point, but with the exception of John McMahon, our intelligence community leadership, and their resource management subordinates, appear to consistly denigrate the value of OSCINT. As so clearly documented in the HAC investigative survey, a survey which included interviews with Ambassadors, Deputy Chiefs of Mission, analysts, and other key personnel around the globe, "without exception, the consensus is that unclassified media are the single most important source of valuable intelligence information" (emphasis in original); as quoted in the Marling memorandum, supra note 7, pages 1 and 4. The same HAC report noted that the various recommendations in the McMahon-approved Open Source Action Group (OSAG) report "have either been ignored or are being implemented perfunctorily on an ad hoc basis or parochial basis." It is evident that the current attempts by the existing Open Source Task Force are a continuation of this trend of ignorance, and offer little hope for radical improvement.

The need for such a strategy is compelling, and has three underpinnings:

(1) We can no longer afford to rely almost exclusively on very expensive and difficult to process technical collection capabilities; the budget deficit and the Congressional imperative that we do more with less requires that we seek alternative means;

(2) The emerging threats are predominantly in the open --we are not proscribed by organization or secrecy from understanding these threats, but rather by our own lack of organization and interest; and finally;

(3) OSCINT provides both an order of magnitude increase in our return on investment strictly from the collection/analysis point of view, and an order of magnitude increase in our return on investment in terms of its utility and exploitability through sharing within government, with coalition forces, and with U.S. industry and the academic community.

OSCINT provides both an order of magnitude increase in our return on investment strictly from the collection/analysis point of view, and an order of magnitude increase in our return on investment in terms of its utility and exploitability through sharing within government, with coalition forces, and with U.S. industry and the academic community.

The government cannot resolve these deficiencies alone; a concerted cooperative effort with industry and the academic community will be required, and should ultimately include foreign and international organizations. As an immediate interim measure, this report addresses the requirement for a cooperative government-business-academic CEOS.

OSCINT, in short, is an alternative paradigm, a "new paradigm" from within which we can approach the task of devising a new National Security Act and a new national intelligence structure.

MILITARY CONSUMER'S VIEWPOINT

The majority of our national consumers for intelligence, particularly in the military, have--at best--a SECRET clearance, and more often than not in these days of increased security concern, no active clearance at all.

Most consumers do not have Sensitive Compartmented Information (SCI) or Top Secret (TS) clearances. Many of the consumers who do have such clearances do not have the time or the inclination to read compendiums of SCI information. The majority of our national consumers for intelligence, particularly in the military, have--at best--a SECRET clearance, and more often than not in these days of increased security concern, no active clearance at all. This is particularly the case with our single most important military consumers, the platoon commanders and pilots. While eligible for a SECRET clearance, most are not technically eligible for SCI products. All would prefer unclassified information that could be shared with their fellow officers, their troops, and allies as required.

The consumer's point of view at the policy level has been ably articulated by such individuals as Sumner Benson²¹ and Robert Blackwell²². More recently, both at the Department of the Navy's Technology Initiatives Wargame 1991²³, and within the

²¹ Sumner Benson, a former CIA employee who has served as a senior civil servant in DoD, has for several years shared his insights with students in the CIA-sponsored "Intelligence Successes and Failures" course. Benson clearly articulates the policy-makers lack of time and competing sources, as well as the lack of clearances within the policy-maker's staff. "A SECRET paragraph is better than an SCI page...your primary competition is the Post."

²² Robert Blackwell, a former Deputy Assistant Secretary of State and member of the National Security Council staff, has briefed participants in the twice-annual "Intelligence Policy Seminar" sponsored by the Intelligence Producers Council at Harvard's John F. Kennedy School of Government. His remarks are consistent with those of Sumner Benson.

²³ See the section on military wargames for details focusing on intelligence and related shortfalls. The Navy wargame identified OSCINT as the single most important priority to be addressed by the national intelligence community--such a

...the four principal groups of military consumers (are the) department, defense agency, and service planners and programmers... theater commanders-in-chief and their staffs...tactical commanders and their staffs...(and the) technical acquisition managers and system designers...

United States Marines Corps²⁴, the urgent unmet requirements for a dramatic increase in OSCINT, as well as a radical change in the manner in which the intelligence community as a whole organizes its electronic databases, have been publicly articulated and endorsed by a broad cross-section of consumers.

It helps to distinguish the four principal groups of military consumers, consumers whose needs are not now being adequately met by existing national and defense intelligence products and their supporting electronic system architectures:

(1) Department, defense agency, and service planners and programmers responsible for training, equipping, and organizing military forces;

finding is hardly consistent with suggestions that the OSCINT situation is "by and large" well in hand. Army findings, as developed in its own technology wargames in 1990, support the need for a new paradigm for intelligence.

²⁴ Besides articles by the (then) Commandant of the Marine Corps and a member of his staff, the Marine Corps has recently completed its first annual call for intelligence production requirements. Fleet Marine Force requirements, notably from various independent Marine Air Ground Task Forces in the Fleet Marine Force, stressed the unfulfilled requirements for unclassified military intelligence products on both conventional and non-conventional forces. In DESERT STORM/ DESERT SHIELD, and in such humanitarian operations as SEA ANGEL in Bangladesh, Marine Corps general officers and their staffs learned that unclassified products were absolutely essential as a means of satisfying both their internal operational requirements for readily disseminable and exploitable materials, and for sharing with coalition partners and international non-governmental organizations. As the Marine Corps prepares to deal with emerging threats and rapidly changing ad hoc coalitions formed for crises of short duration, the Marine Corps' need--representative of the broader DoD need--for OSCINT products will increase.

(2) Theater CINCs and their staffs responsible for planning and employing earmarked forces throughout specific regions;

(3) Tactical commanders and their staffs responsible for planning and executing specific contingency missions; and

(4) Technical acquisition managers and systems designers responsible for developing systems, defeating countermeasures, and (in theory) ensuring that technical systems are appropriate to the probable environments within which they will be employed.

The most important consumer group in terms of long-term resource conservation and sound national fiscal strategy is the department, defense agency, and service planner & programmer constituency. This group, comprised of representatives from each Service--and the department and defense agency civilians who provide oversights in their respective areas of responsibility--plans and programs for the training, equipping, and organizing our forces, and for related capabilities of common concern. It is this group that considers the mid-term and long-term threat, determines what capabilities are required, and then sets in motion the lengthy and extremely expensive process of defense acquisition.

Most of the people in this group do not need classified intelligence to fulfill their responsibilities. Many will argue this point, but it is important to distinguish between the need to decide what level of capability one requires, and the need to actually understand the technical details of opposing systems. It is also essential to understand that many top-level policy-makers who do have SCI clearances do not have the time to read compendiums of SCI information, while their gatekeepers, those who screen incoming materials, may not have SCI clearances at all.

At the strategic level, it is far more important for planners & programmers to have an appreciation of the general situation, and to an extent of the regional situation, for each of the different defense missions areas:²⁵

²⁵ Defense mission areas are distinct from the defense intelligence functional areas, and represent predominantly technical areas of interest pertaining to different kinds of military capabilities. At all levels of analysis, the national and defense intelligence communities have tended to focus solely on the technical intelligence aspects of each mission area, and have failed to adequately convey the realities of operational geography and civil factors (e.g. bridge loading data) which frequently make technical lethality issues secondary if not irrelevant.

The mission areas of concern to the Marine Corps are reproduced below as a means of illustrating the scope of our interest, and making obvious the degree to which such mission areas can be illuminated through open source research and analysis:

- MA-11 Command & Control
- MA-12 Intelligence
- MA-13 Security
- MA-15 Special Operations
- MA-22 Ground Tactical Mobility/Countertermobility
- MA-23 Close Combat
- MA-24 Fire Support
- MA-32 Antiair Warfare
- MA-33 Assault Support
- MA-34 Offensive Air Support
- MA-35 Control of Aircraft, Missiles, and Remotely Piloted Vehicles
- MA-36 Electronic Warfare
- MA-41 Supply
- MA-42 Maintenance
- MA-43 Transportation
- MA-44 Expeditionary Engineering
- MA-45 Health Services
- MA-46 Services

Much if not all of the information we need to support the Concept-Based Requirements System (CBRS) can be established through OSCINT, and has the added advantage of being easily exploitable in the over-all Planning, Programming, and Budgeting System (PPBS) with its numerous requirements for on-going justification within the Executive and to various Congressional committees. It merits comment that the strategic planners and programmers are not warfighters--they do not have a critical requirement for classified operational intelligence other than to keep current in order to support the warfighters and advise the policy makers.

It merits comment that the strategic planners and programmers are not warfighters--they do not have a critical requirement for classified operational intelligence other than to keep current in order to support the warfighters and advise the policy makers.

Three examples of the kind of unclassified strategic generalizations that should be provided by the intelligence

community to this consumer group are provided below²⁶:

(1) Ground mobility. Much of the Third World does not permit the kind of cross-country mobility that is required for off-road maneuver. Most of the Third World also appears to have such a limited transportation infrastructure (lines of communication), with poor roads and bridges generally able to handle 30-40 tons, that one strategic generalization that quickly emerges is that pertaining to the weight and size of ground mobility systems. If Service planners and programmers had been given an adequate appreciation for these factors, an appreciation that the Marine Corps has easily developed using only unclassified sources, it is unlikely that the M1A1 tank and the M-198 systems would have been so uncritically received.

(2) Air mobility. Much of the Third World sees sustained temperatures above 80 degrees Fahrenheit, what would be called a "hot" day in aviation circles...yet most aircraft are designed for "warm" days and provide their optimal performance in the 60-70 degree range. This means that our forces operating in the Third World will be obliged to use aircraft whose lift and range will be constrained. This has particularly serious implications for theater lift and for "maneuver from the sea" concepts of operation calling for over-the-horizon launches.

(3) AIDS. This is a strategic generalization our planners and programmers have not yet begun to address. The issue is: to what extent is AIDS so prevalent in the Third World that any U.S. force planning to render disaster relief should be equipped with AIDS protective clothing and other measures? How to troops handle mass casualties, most infected with AIDS, without bearing an unacceptable degree of risk of contagion?

²⁶ Most of the examples used in this report are drawn from the Marine Corps experience because this Service, in standing up a new National Foreign Intelligence Program production facility, the USMC Intelligence Center at Quantico, Virginia, has devoted two years to the study of alternative means of satisfying its unfulfilled Third World intelligence requirements. It was in the course of doing its first major study, Overview of Planning and Programming Requirements for Expeditionary Operations in the Third World (USMC Intelligence Center, March 1990) that Center personnel, with the assistance of analysts from throughout the community, established the validity of using unclassified to guide major strategic acquisition decisions, and identified a family of products, predominantly unclassified, which could meet the needs of Marine Corps consumers at each level of analysis. The needs of other services can be expected to differ somewhat because of different roles and missions as well as different geographic "universes" upon which generalizations are based, but the approach is a generic one.

...most theater commanders and staff could get along quite well without a great deal of the classified intelligence they receive now, provided they were afforded an adequate OSCINT capability.

At the theater level, while the focus on specific regions narrows the "universe" from which unclassified generalizations can be constructed, most of what is required in peacetime can still be met through a review of open sources and the production of OSCINT. At the theater level, besides monitoring general orders of battle (OOB), readiness, and sustainability of potentially hostile military capabilities, there is an increased interest in the opportunities and constraints afforded by operational geography and civil factors. Again, most of these requirements can be satisfactorily fulfilled through well-planned monitoring of open sources. There is no substitute for classified collection assets and carefully defined classified production and dissemination, particularly in the indications & warning (I&W) arena, but the point must be reiterated: most theater commanders and staff could get along quite well without a great deal of the classified intelligence they receive now, provided they were afforded an adequate OSCINT capability.

At the tactical level, there are three aspects to consider: training, planning, and liaison.

At the tactical level, there are three aspects to consider: training, planning, and liaison. In the training arena, classified intelligence is simply not useful. More than one commander has stated their need for unclassified recognition manual and "how they fight" reference manuals, including "Intelligence Preparation of the Battlefield" templates²⁷. Most

²⁷ Intelligence Preparation of the Battlefield (IPB), a very useful doctrine for understanding the employment of conventional forces and establishing intelligence requirements consistent with likely dispositions and employment patterns, was developed by the U.S. Army. It has yet to be applied to non-conventional forces (e.g. narco-terrorists, Third World paramilitary forces, and insurgent groups) in part because "methods" often presuppose that the enemy is going to have a pre-determined order of battle and pre-determined methods of

troops, including the Non-Commissioned Officers (NCO) responsible for the bulk of their training, are not eligible for clearances for lack of a background investigation. Most officers, especially junior officers in troop-leading positions, while eligible for clearances because of the required Basic Investigation (BI), do not have active clearances for SECRET, much less TS information. The training requirement must be met with unclassified information.

The planning requirement should ideally be met through a combination of unclassified and SECRET information. Most TS/SCI is simply too cumbersome and voluminous (without commensurate relevance to the task at hand) to be useful, and will in many cases be ignored, even by those who do have the requisite clearances.

The liaison requirement, now met in wartime through the extensive and relatively arbitrary waiver of dissemination restrictions, needs to be satisfied in peacetime as it would be in wartime.²⁸ Throughout the world the military needs unclassified commercial alternatives to existing intelligence resources--this need is particularly urgent in the imagery and the mapping, charting, & geodesy (MC&G) arena. Such unclassified materials are essential as a means of establishing common concepts, doctrine, and operating procedures with allies, many of whom are allies for unanticipated contingencies of short duration (e.g. disaster relief).

The technical acquisition and system design requirements for intelligence support three aspects: system capability, defeat of countermeasures, and environmental conditions which include both the regional or global prevalence of the system and counter-systems, and the operational geography or civil factors which

fighting. Perhaps the greatest challenge facing tactical intelligence analysts, however, is that which combines the need to rely on OSCINT, and the fact that most of the emerging threats are "ad hoc", often random in nature, and not associated with previously recognized governments or conventional forces.

²⁸ During TIG-91 the operators in the INTEL Cell, including a Marine Colonel, a Navy Wing Commander who led the lead flight in DESERT STORM, and a Navy Captain (O-6) playing the role of theater CINC were adamant in their requirement for unclassified information, both for use with our own personnel without clearances, and for immediate sharing with coalition partners. They were insistent that we should "train as we fight" and that the data bases and standard families of products should include unclassified products (imagery as well as text) that do not require "in extremis" waivers to disseminate to uncleared personnel.

facilitate or constrain system employment.

In denied areas there is no question but that selected aspects of enemy system design and doctrine must be the subject of classified reporting. The same is true of countermeasures. In most of the world however, this information is readily available through industry publications. Environmental conditions, including such factors as bridge loading data, is generally available in unclassified publications, including "gray literature", but not routinely exploited by the community.

MILITARY PRODUCER'S VIEWPOINT

There is a prejudice within the intelligence production community against the use of open source information. This prejudice, while understandable in the context of the various cultures of secrecy characteristic of the intelligence community, is unreasonable given the consumer's desire for unclassified products, the relative cheapness of open sources, and the extraordinary availability of open source information.

The producer is faced with a dilemma in dealing with OSCINT.

On the one hand, the entire national intelligence community has spent every year since its inception in 1947 developing covert technical and clandestine human collection capabilities. Although the collection management process provides for OSCINT tasking²⁹, the individual analyst and production manager has an easier time of it if they channel their tasking through the traditional disciplines of HUMINT, Imagery Intelligence (IMINT), and Signals Intelligence (SIGINT). One obvious disadvantage of this organizational arrangement is that unclassified information will often be classified solely in relation to its collector, and may or may not be disseminated to others.³⁰

On the other hand, the individual analyst, even if they have the capability to exploit open sources through their reference librarian or through direct communication with the Country Team, generally will not have the knowledge or the time to review the vast quantities of materials even if they were provided at his or

²⁹ The Foreign Intelligence Priorities Committee (FIPC) maintains a comprehensive U.S. Foreign Intelligence Requirements Categories and Priorities (FIRCAP) document which is updated monthly and reviewed in its entirety annually. FIRCAP priorities are "generic" and not discipline-specific.

³⁰ For a review of information pathologies and potential technical solutions spanning the strategic and tactical gamut between the Country Team, the theater, and parent organizations at the national level, see Robert D. Steele, National Security C-I-H: A Strategic and Tactical Information Management Perspective (University of Oklahoma, Programs in Public Administration, May 1987).

her desk, and would in any case be discouraged from excessive attention to open sources as opposed to classified sources³¹.

...blind assumption that classified sources were "by definition" the only reliable sources...

...until today what no one has really called into question was the relative value of open sources as opposed to covert technical sources and clandestine sources...we have now reached a point where this is the issue to be addressed...

There is a prejudice within the intelligence production community against the use of open source information. This prejudice, while understandable in the context of the various cultures of secrecy characteristic of the intelligence community, is unreasonable given the consumer's desire for unclassified products, the relative cheapness of open sources, and the extraordinary availability of open source information.

To an extent, the consumers have permitted this prejudice to become entrenched because of their blind assumption that classified sources were "by definition" the only reliable sources, and their lack of understanding of the diversity and utility of open sources. Despite past studies emphasizing the value of open sources, until today what no one has really called into question was the relative value of open sources as opposed to covert technical sources and clandestine sources...we have now reached a point where this is the issue to be addressed.

³¹ Analysts discussing this problem in one running of the "Intelligence Producer-Consumer Course" offered regularly by the CIA commented that there was actually managerial disdain and potential retribution to be considered if analysts were routinely seen reading unclassified literature at their desk. A senior analyst, writing for Studies in Intelligence, has also noted that much of what analysts provide the policy maker is over-classified because of one SCI tid-bit--we need to seriously rethink how we present intelligence, and get away from practices which unreasonably constrain exploitation.

MILITARY COLLECTOR'S VIEWPOINT

Each of the three major disciplines, HUMINT, IMINT, and SIGINT, has major shortfalls in their capability to collect open source information. These shortfalls cannot be resolved by the government acting unilaterally...

It is difficult for collectors to take OSCINT seriously when their entire culture, their precepts for promotion as well as their informal social standing, is founded on the collection of classified information. This is particularly the case when most HUMINT collectors are outside the military domain, and the remaining collection assets are dominated by the priorities of national policy makers.

Each of the three major disciplines, HUMINT, IMINT, and SIGINT, has major shortfalls in their capability to collect open source information. These shortfalls cannot be resolved by the government acting unilaterally--only a cooperative effort with the private sector, and ultimately foreign organizations--will enable the creation of a global all-source data collection infrastructure.

The HUMINT arena offers a clear-cut example of a hierarchy in which those responsible for OSCINT are at the bottom. The fact is that in the world of clandestine operations, with its distinctions between denied, internal, covert, and specialty targets, those who are "declared" and those who are "overt" are at the bottom of the pecking order. When this state of affairs is exacerbated by an institutional reluctance to deal with military requirements, and a top-level management refusal to provide adequate priorities for Third World requirements, the dramatic shortfalls in overt collection against Third World military contingency requirements can be readily surmised.

There will be those that disagree with this representation, but the fact is that in DESERT STORM/DESERT SHIELD it took a heroic effort on the part of the domestic HUMINT cadre to obtain the intelligence needed for precision targeting against C³ and infrastructure nodes--intelligence which could have been available, should have been available, and would have been

available had domestic collection efforts kept pace with requirements.³²

The above personal and speculative account if offered for illustration purposes only. A more substantive review of exact manning and dollar allocations should make very clear where the HUMINT community places its priorities, while also documenting the severe shortfall in overt HUMINT collection against Third World collection priorities.

In the IMINT arena, there are severe shortfalls in our government-owned imaging capability (e.g. broad area search, short-notice search, and synoptic coverage necessary for mapping), as well as in our ability to take advantage of commercial imagery services, and an active policy--the 10 meter resolution limitation--which directly³³ constrains the value of commercial services to the military.

³² Even when the data is collected as a matter of routine, it is often discarded or stored in a manner which makes it irretrievable. The USMC Intelligence Center investigated the availability of Third World bridge loading data, and learned that while defense attaches routinely submit detailed reports, including hand-held photography, much of their reporting is either discarded or stored in warehouses.

³³ As established by a USMC Intelligence Center study, supra note 26, the fact is that we do not have the mapping, charting, and geodesy (MC&G) data--or the related precision targeting data--for most of the Third World. According to one study, completed in 1989, of 67 countries and two island groups of interest to the Marine Corps, twenty-two have no maps, and would require rapid exploitation of multi-spectral imagery with grid overlays. Mexico, Surinam, Bangladesh, Greece, and Turkey are in this category. An additional thirty-seven have only some 1:50,000 tactical maps, generally for the major ports and cities, and generally very dated (i.e. not showing roads, airfields, and other man-made features established in last ten years or so). Colombia, most of Central America, Peru, and most of our countries in Southwest Asia, Africa, and Asia fall in this category. Only ten of our sixty-nine areas of interest have complete 1:50,000 coverage, and that coverage is old, generally at least ten years out of date. This is a major reason why the Marine Corps must strive to obtain national and defense intelligence support for the privatization of our most urgent tactical mapping needs, which can be met by using multi-spectral imagery (MSI) with grid overlays. However, the existing 10 meter resolution restriction on domestic MSI products severely degrades our capability and by consensus of the TIG-91 INTEL Cell, must be retracted. Our lack of precision targeting data (e.g. precise locations of specific buildings, floors, and rooms or electronic

In the SIGINT arena, defined to include video broadcasts, there is no well-established capability to collect, process, and disseminate open source broadcasts, nor any structure for obtaining, cataloging, and exploiting the wealth of archived tapes produced by organizations such as Cable News Network (CNN).

equipment suites) is even more severe.

SURVEY OF EXISTING CAPABILITIES--MILITARY VIEWS

THE SERVICE INTELLIGENCE CHIEFS, THE THEATER CINCS, AND THE DEFENSE INTELLIGENCE FUNCTIONAL MANAGERS SHOULD BE ASKED TO CONTRIBUTE TO THIS SECTION. NO REPORT SHOULD BE PUBLISHED WITHOUT SPECIFIC INPUT FROM THESE CONSUMERS AND THEIR NON-MILITARY COUNTERPARTS IN THE REMAINDER OF THE GOVERNMENT

MILITARY WARGAME RESULTS

Technology is not the show-stopper--management is where we must change the way we do business.

Our number one intelligence requirement should be the development of open source multi-media multi-level security systems (to include fostering of commercial and foreign capabilities through international standards).

Highlights

Below are highlights from the Technology Initiatives Game 1991 (TIG-91) "scrub" of COPENICUS (Navy Space and Electronic Warfare (SEW) architecture, no expansion), and a brief summary of key C3I points from a related wargame, Global War 1991.³⁴ The language which follows is extracted directly from the official Marine Corps trip report; all emphasis is additive and highlights findings of the wargames of greatest significance to OSCINT.³⁵

Vice Admiral Reynolds, Director, Test and Evaluation and Technology Requirements, reported the following key TIG-91 judgements to the Chief of Naval Operations:

(1) "Technology push is not the major issue...our most difficulty challenge is management of fast moving technology.

³⁴ The Technology Initiatives Wargame 1991 took place at the Naval War College 21-25 October 1991, and included participants from throughout the intelligence and communications communities of the government. Three cells were exercised in support of a policy cell of flag officers: an Operations Cell, a C3 Cell, and an Intelligence Cell. Each cell in turn was divided into National, Theater, and Tactical Sub-Cells. Global War 1991 took place at Newport in June 1991. The Army's Technology Base Seminar Wargame took place at two different locations 23-26 April 1990 and 6-8 June 1990; although not cited here its results were consistent with the findings of the Navy-Marine Corps wargames.

³⁵ Marine Corps Trip Report: Technology Initiatives Wargame 1991 (21-25 October 1991); approved for dissemination by the AC/S C4I2 on 3 January 1991, the trip report was a collaborative effort by Mr. Ronald Elliott (SES); Cols Black, Lindblom, Mastrion, Smith, and Stankosky; LtCols Reager and Work; and Mr. Robert D. Steele.

(2) Open architectures facilitating use of commercial standards and formats is imperative.

C4I2 progress must be made in three areas: architectural, doctrinal, and technical; of these, the greatest progress at least expense can be made in the doctrinal area, followed by the architectural.

Technology is not the show-stopper--management is where we must change the way we do business.

Architecturally we must define a new paradigm of what information we need, how we handle it, and how it is delivered to the user; this new paradigm must include an information architecture (vice a system/command architecture) approach, must extend to include commercial and coalition capabilities, and integrate Geographic Position System (GPS) data.

Doctrinally we need to ensure we are represented in joint and other service "doctrine" forums. Cost will not be an impediment to progress--lack of innovative management at all levels is the show-stopper. We need a new approach to C4I2, both as functional mission area and as a new and powerful form of warfare. While some might not agree, many would suggest our new concepts must integrate unanticipated short-term coalitions, media operations, C4I2 oversight over weapons system design and employment concepts, new data requirements associated with precision targeting, unclassified data requirements necessary for real-time and coalition operations, and a very broad understanding of needed developments in concealment, deception, and covert communications capabilities suited to future adversarial C4I2 capabilities.

Technically the short-term emphasis should be on cross-theater, cross-service improvements in processing and dissemination applications that provide for standardized transparent access to multi-media data at multiple levels of security. In the mid-term, exploitation of open sources and commercial capabilities must be addressed. Over the longer term, cheap multi-discipline satellites, Identification of Friend or Foe (IFF) down to man/machine level, and portable C4I2 system for Marines should be priorities.

Intelligence Priorities

INTEL Cell investment priorities established early on in TIG-91 included, in this order as reported to the flag panel:

(1) Open source multi-media multi-level security systems (to include fostering of commercial and foreign capabilities through international standards)

(2) Automated all-source correlation system with integrated advanced/artificially intelligent processing and analysis tools (merge functionality of the CIA's CATALYST with Navy COPERNICUS and Marine Corps Tactical Automated Command and Control System (MTACCS) architecture)

(3) Information (database) architecture, multi-media in nature (start doing data driven system design)

(4) National all-source automated intel'igence requirements and collection management system (integrate foreign intelligence priorities committee, disciplinary committee priority documents, and JCS intelligence priorities into a single coherent system which provides accountability and auditing capability to determine customer satisfaction)

(5) Cheap pop-up satellites, all-weather, multi-discipline

(6) Computer penetration technology across the board

(7) Virtual reality/multi-media alteration capabilities including truth validation

Intelligence Investment Strategies

The basic investment strategies related to these priorities and recommended by the INTEL Cell to the flag service included, in this order:

(1) Maximize inter-operability with commercial systems and products

(2) Facilitate/push international standards

(3) Use unclassified sources to maximum extent possible, particularly in building Third World encyclopedic database

(4) Plan for and develop capability to automatically sanitize all intelligence to any level of classification (operators in cell expressed very strong desire to "train as we fight" and create data structure now)

(5) Use Integrated Services Digital Network (ISDN) as core of coalition C4I2 approach

Intelligence Architectural Issues & Highlights

The key INTEL Cell architecture issues & highlights were:

(1) At the National Level: shift to an information architecture vice a system architecture; enforce, nurture, and

pursue use of commercial and international standards

(2) At the Theater Level: include coalition connectivity and classification constraints in architecture

(3) At the Tactical Level: establish global multi-media dissemination capability (to any vehicle/man)

Intelligence Doctrine Issues & Highlights

The key INTEL cell doctrine issues & highlights were:

(1) At the National Level: establish unclassified alternative databases & products suitable for broad dissemination to unclassified operators and sharing with allies; completely redefine precision targeting database needs and carry out pre-contingency database fill; develop national knowledge warfare concepts & plans; redefine & realign HUMINT to support contingency planning and execution

(2) At the Theater Level: develop Low Intensity Conflict (LIC) I&W methods and data elements; develop theater doctrine changes integrating new C3I precision targeting methods into campaign planning

(3) At the Tactical Level: remove 10M resolution constraint on U.S. commercial imagery; develop media interaction methods and military occupational specialties; develop collection rules of engagement (ROE) for multi-belligerent pre-war situations (i.e. outlining ROE for C3CM in deterrence phase)

Intelligence Technology Issues & Highlights

The key INTEL Cell technology issues & highlights were:

(1) At the National Level: install open source exploitation capabilities throughout community; develop single national automated data correlation capability (multi-media with time and location tags on all data to facilitate fusion); develop pop-up satellites for contingencies

(2) At the Theater Level: pursue "man in space" and "man on site" capabilities

(3) At the Tactical Level: develop multi-sensor battle damage assessment tools for near-real-time battle damage assessment from original delivery platform (e.g. improved gun sensors); develop technology enhancers for covert and clandestine HUMINT--sustained SATCOM power, life support systems; develop generic advanced workstation (a multi-level, multi-media, multi-window toolkit which allows an analyst to enter a seamless world of data regardless of level of classification or media type)

"Global War 1991" Intelligence Issues & Recommendations

At Global War 1991, a few intelligence "issues" and recommendations were in various working papers or emerged in discussion:

(1) Importance of coalitions to warfighting as well as peacetime engagements absolutely requires a well-developed capability for sanitizing, sharing, and disseminating intelligence to allies (including short-term allies and non-governmental organizations)

(2) Importance of intelligence as the trigger for reconstitution of forces cannot be exaggerated (yet there is little support for fencing intelligence so it can provide the advance warning needed)

(3) Clear concern over lack of warning capability on destabilizing events including non-military trends and occurrences (warning capabilities needed to trigger reconstitution of forces for Third World regional wars do not exist and will take years to build)

(4) Increased emphasis required on HUMINT, on analysis even if at expense of collection, and on maintenance of databases in non-traditional areas including trade, environment, medical, and demographic

(5) Absence of joint doctrine on intelligence, particularly as it might refer to coalition operations and support to law enforcement or to non-governmental disaster relief operations, continues to constrain planners

The Army Need for a Paradigm Shift

The Army Technology Wargame identified a major C3I programmatic implications which should bear on the community approach to OSCINT: "The problem with C3I is not one of low visibility or funding, but the challenge of an overall architecture for sensors, processing, and communications. Such an architecture exists for Division and above, and for individual weapons systems, but the intermediate structure is extremely diffuse. The key to ALBF is the efficient delivery of information, tailored to the recipient, wherever [and whenever] it is needed. Current approaches focus on automating existing manual processes, and linking those processes that have always communicated. ALBF may require the Army to alter this paradigm." (emphasis added)

SURVEY OF UNFULFILLED MILITARY OPEN SOURCE REQUIREMENTS

THE SERVICE INTELLIGENCE CHIEFS, THE THEATER CINCS, AND THE DEFENSE INTELLIGENCE FUNCTIONAL MANAGERS SHOULD BE ASKED TO CONTRIBUTE TO THIS SECTION. NO REPORT SHOULD BE PUBLISHED WITHOUT SPECIFIC INPUT FROM THESE CONSUMERS AND THEIR NON-MILITARY COUNTERPARTS IN THE REMAINDER OF THE GOVERNMENT

CONCLUSION

The few additional details contained in the second Executive Summary (e.g. Presidential Blue Ribbon Commission) do not need elaboration.

OSCINT as a capability is too important to be given such short shrift as has been the case with the initial draft report to the DCI.

We recommend that the report be properly classified (i.e. not be classified); that it at least be staffed to all intelligence community principals as well as government and private sector consumers and producers; and that a significantly expanded working group take on the task of developing a serious and comprehensive plan--including detailed manpower and resource requirements--for establishing a national knowledge management strategy and a related information technology initiative.

In order to better fulfill the expanded task, we recommend that an entirely new Task Force be constituted, under the leadership of the Administrator of the Defense Technical Information Service (DTIC), and with the assistance of elements of the intelligence community. This is one instance when the intelligence community does not have the internal expertise to fully define the requirements and the needed capabilities. A complete report, to include detailed manning, funding, and facilities requirements, as well as program objectives and milestones, can be ready within ninety days of commission.

BIBLIOGRAPHY

- Benson, Sumner, Presentation to "Intelligence Successes and Failures" Course, Office of Training and Education, Central Intelligence Agency, 16-23 October 1987
- Blackwell, Robert, Presentation to "Intelligence Policy Seminar", John F. Kennedy School of Government, Harvard University, 8-14 December 1991
- Carver, George A. Jr., "Intelligence in the Age of Glasnost", Foreign Affairs (Summer 1990), pages 147-166
- Center for Naval Warfare Studies, "Global War 1991", Naval War College, July 1991
- _____. "Technology Initiatives Wargame 1991", Naval War College, 21-25 October 1991
- CIA, Open Source Exploitation Program (March 1986), approved by then Acting DCI John McMahon (S/NF)
- Foreign Intelligence Priorities Committee, U.S. Foreign Intelligence Requirements Categories and Priorities (FIRCAP, S/NF)
- Gray, Alfred M., "Global Intelligence Challenges in the 1990's", American Intelligence Journal (Winter 1989-1990), pp. 3-7
- Hahn, Samuel and Don Parrish, CATALYST: Sketching the Steps Toward an Integrated Computing Environment for Analysis (CIA/DI/OSWR, October 1991)
- Hall, Keith, "Challenges Faced by U.S. Intelligence", American Intelligence Journal (Summer/Fall 1990), pages 1-3
- House Appropriations Committee, "Exploitation of Unclassified Media for Intelligence Purposes", Report of the Surveys and Investigations Staff, 15 March 1989, S
- HUMINT Committee, Directory: Information Resources Based on Foreign Media and Publications (DCIC 10006-85, HC 85-207, July 1985, FOUO)
- HUMINT Committee, Directory: Information Resources Based on Foreign Media and Publications, Annex (DCIC 10007-85, HC 85-208, July 1985, S/NF)
- Information Handling Committee, "Establishment of the Centers for Ocean Surveillance and Maritime Information Coordination (COSMIC)" (Draft Concept Paper, Fax dated 15 March 1991)

_____. "Open Source Handling/Exploitation and/or Information Handling" (Draft, never signed, S/NF)

Intelligence Producers Council, Report on Automated Open-Source Data Bases (Draft August 1990, final due out April 1991, S/NF/NC)

Marling, George L., "HAC Staff Report on Open Source Exploitation" (Memorandum for the Record dated 6 November 1989, S)

MITRE Corporation, Open Source Processing Research Initiative (OSPRI), Draft MITRE Technical Report, 6 January 1992

Muzbeck, K. and M.B. Garnot, "Establishment of Electronic Open Source Exploitation Capabilities for Quantico Community; Enhancements to Existing Breckenridge Library Funded by Intelligence" (Memorandum dated 4 April 1989)

Open Source Information Exchange Working Group, "Open Source Information Exchange (OSIX) Concept of Systems Design and Operations" (Draft dated 10 March 1989, S)

Open Source Task Force, "Open Source Task Force Draft Report" dated 27 December 1991

_____. "Joint Open Source Task Force Report and Recommendations", Working Group Draft dated 6 January 1992

Reilly, Lucy, "Bush Shift Adds Tech to Agenda: Cabinet, Industry to Craft National Policy", Washington Technology (9 January 1992), page 1

Steele, Robert D., "Applying the New Paradigm: How to Avoid Strategic Intelligence Failures in the Future", American Intelligence Journal (Autumn 1991), pages 43-46

_____. "Intelligence in the 1990's: Recasting National Security in a Changing World", American Intelligence Journal (Summer/Fall 1990), pp. 29-36, esp. p. 30-33.

_____. "Intelligence Support for Expeditionary Planners", Marine Corps Gazette (September 1991), pages 73-79

_____, National Security C³I³H³: A Strategic and Tactical Information Management Perspective (University of Oklahoma, Programs in Public Administration, May 1987)

USMC Intelligence Center, Overview of Planning and Programming Factors for Expeditionary Operations in the Third World (Expeditionary Environment Study 1-89; Vol I: Briefing,

Vol II: Supporting Data, Vol III: Country Book; Final
Report March 1990)

Webb, Diane Q., CATALYST: A Concept for an Integrated Computing
Environment for Analysis (CIA/DI/OSWR, October 1989)

OSCINT POINTS OF CONTACT

NOTE: The list below includes only the most obvious starting points, and does not include the members of individual working groups such as those supporting the STIC and various ICS committees. It also does not include the defense intelligence functional manager, the theater J-2s, the service intelligence chiefs, members of the Council of Defense Intelligence Producers (CDIP), and other critical points of contact for establishing the minimal mandatory OSCINT requirements and capabilities for the military (to include humanitarian assistance considerations).

ALLEN, Kenneth	Sr VP Info Indus Asso	(202) 639-8262
ANDERSON, James	Security Consultant	(215) 646-4706
ANDRIOLE, Stephen	DARPA, AI, DIA, Drexel	(215) 895-2491
BERBRICH, John	ADD/DIA (S&T)	(202) 373-4827
BRIGGS, Charles	Former ExecDir CIA, ESG	
BROMLEY, Allen	Dir OSTP	
CAPONIO, Joseph	DepDir NTIS	(703) 487-4612
CHARVONIA, David	ExecScty IRDC	(202) 376-1077
CIRILLO, Fred	STIC Chairman	
CLARK, Joseph	DepDir NTIS	(703) 487-4612
COTTER, Gladys	NASA	(703) 271-5640
DANIEL, Robert	ENERGY DirInt	(202) 586-2610
DOLAN, Karin	USMC Analyst	(703) 640-5865
DORN, Peter	SSCI (TIARA)	(202) 224-1700
ELLIOTT, Randall	DepDir PolMil State	(202) 647-4296
GOLD, David	OMB (NTIS account)	(202) 395-3914
GORE, Albert	Senator	(202) 224-4944
HAHN, Samuel	ESL (CATALYST)	(408) 743-6349
HARRISON, Fred	C/IHC	(202) 376-5560
HENDRICKSON, Tim	FSTS/ASAP	(804) 980-7242
HERRING, Jan	Former NIO(S&T)	
INMAN, Bobby	DDCI, MCC	(202) 456-2352
JOHNSON, Donald	ActDir NTIS	(703) 487-4612
JONKERS, Roy	AIJ, GTE	(703) 818-5947
KEES, Terry	DD/ORD, AIPASG	(703) 351-2565
KEYWORTH, Jay	DirRes Hudson	(202) 333-4800
KINN, Jerry	TASC Bedford	(617) 942-2000
LEAMOND, Nancy	Cong Econ Ldr Inst	
LIND, William	Ctr Cultural Consev	(202) 546-3000
LUKASIK, Steven	STAP, ESG, TRW	

MCMAHON, John N.	Former DDCI	(408)	742-6211
MARLING, George	ExecScy OSC, MITRE	(703)	883-7931
MAUNE, David	Cdr Army Eng Topo	(202)	355-2600
MOLHOLM, Kurt	Administrator DTIC	(703)	274-6800
MORTIMER, Louis	AC/FRD	(202)	245-5290
NALL, Julian	ESG/OSCINT, IDA		
NELSON, Mike	SC(CS&T)	(202)	224-5115
OEHLER, Gordon	NIO/S&T	(703)	482-6811
PEDTKE, Thomas	TechDir, FASTC		
PRIOR, Larry	HPSCI (GDIP/TIARA)	(202)	225-8246
PRONDZINSKI, Jim	TD USCG ICC	(202)	267-2135
RHEINGOLD, Howard	Tools for Thinking	(415)	388-3912
RIDDLE, Niles	D/FBIS	(703)	733-5857
ROBERTS, James	DIRINT OASD(SOLIC)	(703)	693-2896
ROSS, David	OIR	(703)	482-2506
RUH, William	MITRE IR&D	(703)	883-7892
RYAN, Terry	SSCI (GDIP)	(202)	224-1700
SECUNDA, Gary	SOCOM Intel	(813)	830-6396
SLATER, Robert	DIA DIC Dir Rsrch	(202)	373-3342
SPINRAD, Robert	STAP, XEROX	(415)	812-4020
STEELE, Robert	USMC Resource Mgr	(703)	693-5422
VAN CLEAVE, Michelle	OSTP/NS	(202)	395-7326
VAN CREVALD, Martin	USMC Professor	(703)	640-5807
WALLNER, Paul	DIA ODB-3	(202)	373-3105
WATKINS, James	Scty of Energy		
WEBB, Diane	CIA(CATALYST), ESL	(408)	752-2383
WEGMAN, Christine	House (CSS&T)	(202)	225-3651
WEINSTEIN, Jerry	DIA DB	(202)	373-4888
WILLIAMS, James	D/DIA, DIAC, NMIA		
WOTRING, Ray	IPC Staff Chief	(202)	376-5529
YANNUZZI, Rick	OSTP/NS, AIPASG	(202)	395-5052

GLOSSARY

ADP.....Automated Date Processing
AIPA.....Advanced Information Processing and Analysis
ALBF.....AirLand Battle Future

BI.....Bachground Investigation

C3CM.....Command, Control, and Communications Countermeasures
C4I2.....Command and Control, Communications and Computer,
 Intelligence and Interoperability
CATALYST....Computer Aided Tools for the Analysis of S&T
CBRS.....Concept-Based Requirements System
CDIP.....Council of Defense Intelligence Producers
CEOS.....Center for the Exploitation of Open Sources
CINC.....Commander-in-Chief
CNN.....Cable News Network
COTS.....Commercial-Off-The-Shelf

DCI.....Director of Central Intelligence
DGIS.....Defense Gateway Information System
DTIC.....Defense Technical Information Center

ESG.....Executive Steering Group (of the OSAG)

FASTC.....Foreign Aerospace Science & Technology Center
FAX.....Facsimile
FBIS.....Foreign Broadcast Information Service
FCRF.....Federal Contract Research Facility
FIPC.....Foreign Intelligence Priorities Committee
FIRCAP.....(U.S.) Foreign Intelligence Requirements
 Categories and Priorities
FRD.....Federal Research Division
FSTC.....Foreign Science & Technology Center
FY.....Fiscal Year

GPS.....Geographic Position System

HUMINT.....Human Intelligence

I&W.....Indications & Warning
ICS.....Intelligence Community Staff
IHC.....Information Handling Committee
IMINT.....Imagery Intelligence
IPB.....Intelligence Preparation of the Battlefield
IPC.....Intelligence Producers Council
IR&D.....Internal Research & Development
IRDC.....Intelligence Research & Development Council
ISDN.....Integrated Services Digital Network

JNIDS.....Joint National Intelligence Development Staff

LANDSAT.....Land Satellite
 LIC.....Low Intensity Conflict

 MA.....Mission Area
 MC&G.....Mapping, Charting, & Geodesy
 MSI.....Multi-Spectral Imagery
 MTACCS.....Marine Corps Tactical Automated Command & Control
 System

 NCO.....Noncommissioned Officer
 NF.....No Foreign
 NFIP.....National Foreign Intelligence Program
 NIC.....Naval Intelligence Command
 NKF.....National Knowledge Foundation (nominal)
 NSF.....National Science Foundation
 NTIS.....National Technical Information Service

 OIR.....Office of Information Resources
 OOB.....Order of Battle
 OSAG.....Open Source Action Group
 OSCINT.....Open Source Intelligence
 OSIX.....Open Source Information Exchange

 PPBS.....Planning, Programming, and Budgeting System

 ROE.....Rules of Engagement

 S&T.....Science & Technology
 S.....Secret
 SCI.....Sensitive Compartmented Information
 SCIF.....Sensitive Compartmented Information Facility
 SEW.....Space and Electronic Warfare
 SIGINT.....Signals Intelligence
 SNIE.....Special National Intelligence Estimate
 SPOT.....(FR) Earth Observation Satellite

 TIG.....Technology Initiative Game
 TS.....Top Secret

 USG.....U.S. Government
 USMC.....U.S. Marine Corps



DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
WASHINGTON, D.C. 20380-0001

IN REPLY REFER TO:

C4I2R

03 JAN 1992

MEMORANDUM

From: Assistant Chief of Staff, Command and Control,
Communications and Computer, Intelligence and
Interoperability
To: Distribution List

Subj: DISSEMINATION OF TRIP REPORT

Encl: (1) Marine Corps Trip Report: Technology Initiatives
Wargame 1991 (21-25 October 1991)

1. The enclosure is approved for utilization by the participants for information, and may be disseminated by individual participants as desired. No formal dissemination of the report to the Fleet Marine Force or Supporting Establishment is being made by this Headquarters.

D. M. BLACK
By direction

Distribution List:
Mr. Ronald Elliott
Col Douglas Black
Col Stephen Lindblom
Col Robert Mastrion
Col Rod Smith
Col Michael Stankosky
LtCol Richard Reager
LtCol Robert Work
Mr. Robert Steele

"
COPERNICUS MEETS
MTACCS "
"

AO: STEELE DSN 223 5422
EMAIL GICR02

FOR OFFICIAL USE ONLY

MARINE CORPS TRIP REPORT
TECHNOLOGY INITIATIVES WARGAME 1991
NAVAL WAR COLLEGE, NEWPORT RI
21-25 OCTOBER 1991

MARINE CORPS TEAM

Mr. Ronald Elliott	Flag Policy Panel
Col Douglas Black	C3 Cell, National Team
Col Stephen Lindblom	C3 Cell, Theater Team
Col Robert Mastrion	INT Cell, Forces Team
Col Thomas Parrish	INT Cell, Theater Team
Col Rod Smith	OPS Cell, Forces Team
Col Michael Stankoski	OPS Cell, Theater Team
LtCol Richard Reager	OPS Cell, National Team
LtCol Robert Work (PP&O)	C3 Cell, Forces Team
Mr. Robert Steele	INT Cell, National Team

CONTENTS

Introduction.....	1
What Went to the CNO.....	1
Broad Bottom Line.....	1
Admiral Tuttle's Concluding Remarks.....	2
Team Member Observations.....	3
TIG-91 Results.....	6
Flag Panel.....	6
C3 Cell.....	7
OPS Cell.....	9
INTEL Cell.....	11
C4I2 Highlights from Global War 1991.....	14
Army Technology Base Seminar Wargame II Results.....	17
Overall Conclusions.....	20

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

TECHNOLOGY INITIATIVES WARGAME 1991
NAVAL WAR COLLEGE, 20-25 OCTOBER 1991

Introduction

- This report brings together highlights from the TIG-91 "scrub" of COPERNICUS, and provides brief summaries of key points from two related events or documents: the C4I2 portion of Global War 1991 and the Army's Technology Wargame 1990.
- TIG-91 consisted of a flag policy panel and three working cells: C3, OPS, AND INTEL. Mr. Elliott represented USMC on flag panel; each working panel had three Marines--prior coordination ensured that one Marine was assigned to each of the three levels (national, theater, forces) in each cell.

What Went to the CNO

- Vice Admiral Reynolds, Director, Test and Evaluation and Technology Requirements, reported the following three key judgements to the Chief of Naval Operations:
 - "Technology push is not the major issue in SEW/C3; our most difficult challenge is management of fast moving technology."
 - "The COPERNICUS concept needs to be accepted across DoD to be fully successful."
 - "Open architectures facilitating use of commercial standards and formats is (sic) imperative."

Broad Bottom Line

- C4I2 progress must be made in three areas: architectural, doctrinal, and technical; of these, the greatest progress at least expense can be made in the doctrinal area, followed by the architectural.
- Technology is not the show-stopper--management is where we must change the way we do business.
- Architecturally we must define a completely new paradigm of what information we need, how we handle it,

FOR OFFICIAL USE ONLY

and how it is delivered to the user; this new paradigm must include an information architecture (vice a system/command architecture) approach, must extend to include commercial and coalition capabilities, and must integrate Geographic Position System (GPS) data.

- Doctrinally we need to ensure we are represented in joint and other service "doctrine" forums. Cost will not be an impediment to progress--lack of innovative management at all levels is the show-stopper. We need a new approach to C4I2, both as functional mission area and as a new and powerful form of warfare. While some might not agree, many would suggest our new concepts must integrate unanticipated short-term coalitions, media operations, C4I2 oversight over weapons system design and employment concepts, new data requirements associated with precision targeting, unclassified data requirements necessary for real-time and coalition operations, and a very broad understanding of needed developments in concealment, deception, and covert communications capabilities suited to future adversarial C4I2 capabilities.
- Technically the short-term emphasis should be on cross-theater, cross-service improvements in processing and dissemination applications that provide for standardized transparent access to multi-media data at multiple levels of security. In the mid-term, exploitation of open sources and commercial capabilities must be addressed. Over the longer term, cheap multi-discipline satellites, Identification of Friend or Foe (IFF) down to man/machine level, and portable C4I2 system for Marines should be priorities.

Admiral Tuttle's Concluding Remarks

- Commercial reserve, international standards, common bus are part of the solution. Don't hold industry back. Interoperability through commonality. COPERNICUS can be a global system.
- UHF satellites are a weak link, can be jammed.
- Architectures must provide for on-going communications with foes throughout phases of conflict; rules of engagement for C3CM are a critical means of controlling escalation as well as providing for disengagement and deescalation.

FOR OFFICIAL USE ONLY

- Navy has three three-stars working space issues, may add a fourth. Need to change force structure/battle planning perspective, get away from bridge or Washington view and adopt a geographic/global perspective, looking down from space.
- Technical cost is going down in relation to antiquated base; increase of GNP/GNP share as well as cost savings from improved technology and performance will provide ample funding for achievement of COPERNICUS objectives.
- OP-094 wants oversight of combat systems as well as ownership of cryptographic systems, this will allow end to end integration. OP-094 needs to be in the planning phase for every force structure and acquisition effort.
- Must make more progress with data compression, embedded cryptography.
- Submariners and aviators appear on board and fully conscious of COPERNICUS process, need to make headway with surface Navy (and USMC, not mentioned).
- NWP for EW only covers battlegroup, is 99% platform/defensive in nature, focuses on what to report; this must change, is being rewritten.

Team Member Observations

- Mr. Elliott: The Marine Corps group was impressive and made known that you need Marines to win wars. The necessity of integrating the Supporting Establishment, COPERNICUS, and MTACCS information systems was obvious to all. To do so is both a Navy and a Marine Corps responsibility.
- Col Black: This was a significant event because Marines served as the balance from the strategic view to the tactical. Our Marine Corps team members time and time again inspired thought, organized ideas, and tied up loose ends. We played a significant role and should continue to participate in events such as this. They need us and the way we think! The Navy spoke more about joint/combined operations at this event than at any other time I have heard of in the past 22 years.
- Col Lindblom: Although the Marine Corps fielded a top notch team (one SES, six colonels, two lieutenant

FOR OFFICIAL USE ONLY

colonels, and a GS-14), it did not come close to matching the seniority and level of commitment of the Navy or other civilian agencies. USMC needs to establish flag representation capability to handle this kind of requirement.

● Col Mastrion: Two comments:

-- Flag representation need not be from functional area (e.g. AC/S C4I2 personally), but if a flag officer does not participate in an event where so many Navy flag officers are present, this is a de factor insult to the Navy and undermines Navy interest in meeting Marine Corps needs. We must schedule uniformed flag participation in such critical Departmental activities.

-- The civilian side of the intelligence community (both the Central Intelligence Agency and Defense Intelligence Agency) is still not convinced they have a role to play in providing support to operational forces. The two analysts representing those two agencies were simply not listening to the operators in the INTEL Cell. Our intelligence infrastructure must be designed to provide for a total picture, and be part of a coordinated intelligence effort which is not skewed toward the national policy-makers.

● Col Parrish: Development of a sound, flexible information architecture is the principal issue. It is technologically "do-able" but needs a doctrinal foundation. We need flag level guidance on this--and that is going to be hard to get because this is a very difficult area requiring lots of time. MIFASS was left to the C4 community and they did what they could, but it was not good enough. Let's profit from that mistake.

● Col Smith: We must emphasize the Navy/Marine Corps relationship not only in the Joint/DISA environment but within DON. We must eliminate the precept that the Supporting Establishment and the tactical forces, both DoD and DON, are different in standards of interoperability and mission.

FOR OFFICIAL USE ONLY

- Col Stankoski: We've got the technology, just need to manage it; USMC has right structure, good connectivity between programs (including USMC-USN connectivity for COPERNICUS)
- LtCol Reager: Where you sit determines what you see. I don't see SEW as a workable warfare command area. It is a pervasive supporting requirement for true warfighting areas: C2, Fire Support, Ground/Air Combat. The commander is/should be the SEW or C4I2 manager in the sense that he requires critical information upon which to base his decisions. He and his principal staff/subordinate commanders must be able to (1) articulate those requirements, (2) commit the resources to acquire/access/manage the information needed to meet those requirements. Leverage and joint access/participation is mandatory but it alone does not meet internal MAGTF requirements for dissemination/access down to the execution level of warfighting. It is a two part equation, and we must work the internal side as hard as the joint interface side.
- LtCol Work: Space warfare plus electronic warfare does not quite equal SEW. Space certainly supports electronic warfare, as it does anti-surface warfare, anti-submarine warfare, and anti-air warfare. In the Navy, it makes sense to tie space systems and electronic warfare systems programatically. However, the jury is still out on the question of whether or not this marriage is doctrinally and operationally sound. Space warfare is more far-reaching than its implied role in the SEW concept. It is important that the Marine Corps' perception and approach toward space warfare not be dictated by a solution which fits another Service's doctrinal approach to war (i.e. the composite warfare commander doctrine).
- Mr. Steele: Emphasis must be placed on improving the processing and dissemination of what we already get, not on exotic new collection devices. The merging of "product", "data", and "system" has conceptual and doctrinal implications for how we train, equip, organize, and employ forces which are simply not being addressed. We should consider sponsoring a C4I2 Warfare Conference.

FOR OFFICIAL USE ONLY

TIG-91 Results

Flag Panel

● Flag panel issues and highlights:

- C4I2 warfare ("Space and Electronic Warfare"-SEW) will be a major mission area in future, and will be one phase ahead of other warfare areas (e.g demonstration disruptions or international C3I "embargoes" as part of deterrence, already beginning restoration of services as assault phase winds down).
- U.S. must establish national policy regarding commercial communications--to what extent should certain features be mandated? To what extent can legislation and tax relief foster a civil communications reserve capability?
- Coalition warfare will stress C4I2 capabilities; unanticipated and short-term coalition situations require maximum interoperability and standardization along commercial lines, and maximum exploitation of open source or unclassified data for coalition sharing.
- Concepts, doctrine, and rules of engagement for multi-belligerent C4I2 warfare must be developed; C4I2 warfare should come into its own as a separate war-fighting mission area, in some cases a substitute for actual shooting.
- Inter-operability will not just happen if "standards" are adopted; need interoperability verification as part of the acquisition process.

FOR OFFICIAL USE ONLY

C3 Cell

- Following were C3 Cell investment priorities for the 1990's:

- #1 DISN architecture with common operating equipment, standardized protocols, comms loading prioritization, minimal essential comms redundancy
- #2 Surveillance/intelligence capability
- #3 Global navigation/position location reporting
- #4 Mine detection
- #5 Sufficient data transmission capability at all levels
- #6 Counter C3 capability (interruption, disruption, denial, deception, and exploitation)
- #7 Identification of Friend or Foe (IFF) capability to vehicle/man level

- "Hot wash-up" emphasized need for:

- #1 National plans & policy in areas of telecommunications (DOD and commercial), national reserve contingencies (DOD, commercial, international), global connectivity to include foes and non-aligned), United Nations C4I2 policy, national C3CM covert and PSYOP plans, GPS national plan to include common grid for all sensors, and concepts, doctrine for media interaction and exploitation
- #2 Interoperable C3 critical, must include wide area surveillance/battle damage assessment (WAS/BDA) imagery & video, timely coherent tactical picture, common data base with integrity, multi-level security/information security, high volume capability for video & imagery, across joint and combined lines, universal reporting

FOR OFFICIAL USE ONLY

- #3 Dynamic multi-media comms with flexible virtual networks, network management
 - #4 C3-intensive data fusion meet needs in low observable, shallow water anti-submarine warfare, tactical ballistic missile defense, and mine warfare areas
 - #5 Targeting support including WAS/BDA and IFF
 - #6 SEW architecture simulation including technical corollary of "wargame in a box" and training/ planning/contingency tool
 - #7 Need to develop tactical C3 applications of new national systems including multi-spectral imagery, defense surveillance program follow-on, defense data link, sensor to shooter connectivity in near-real-time
- C3 Cell "warfighting strategy" included: PSYOPS campaign, national media plan, use of international commercial assets, information blockade. (Unresolved issues included lack of insertion technology, national-tactical connectivity, survival & security of own C3I, and legality/ methodology of disrupting C3I systems of others including friendly nations sharing transponders with opposition)

FOR OFFICIAL USE ONLY

OPS Cell

● OPS Cell "hot wash-up" briefed eight areas of concern:

- #1 Interoperability--need for policy/management of standards to include open system architecture, common operating environment, joint-level system engineering; and technical measures including gateways and buffers.
- #2 Battle Management--need for policy/management in areas of joint doctrine and command structure; technical measures including sensor netting, classification/identification, and engagement coordination.
- #3 Data/Information Acquisition--need for policy/management of database structure and access; and technical measures including sensor improvements addressing new phenomenologies and need for mobility and focus, integration of expert systems.
- #4 Data/Information Transfer--need for policy/management to achieve integrated strategic-tactical data network and extension of copernicus to joint and combined arenas; technical measures including throughput increase (100-1000X), anti-jamming/secure/covert capabilities, and data compression.
- #5 Data Presentation/Assimilation--need for policy/management to achieve common operating environment, open systems architecture, man-machine interfaces; technical measures including pattern recognition, multi-sensor fusion, and multi-level decision aids.
- #6 Offensive SEW--need for policy/management that is function and force oriented, integrated among command levels; technical measures including soft/hard kill integration, directed energy, low observable/very low observable CCM, and information system penetration capabilities.

FOR OFFICIAL USE ONLY

#7 Information Security--need for policy/management to implement an information security program; technical measures including multi-level security, technical acquisition requirement guidelines, virus inoculation capabilities.

#8 Training--need policy/management commitment to achieve continuous and embedded training; technical measures to provide computer-aided training and simulation as well as cognitive enhancements in all programs.

● OPS Cell conclusions apply to entire game:

- The last word in SEW is warfare
- If it isn't joint and interoperable, we can't afford it
- Enabling technology requires enabling management

FOR OFFICIAL USE ONLY

INTEL Cell

• INTEL Cell investment priorities established early on:

- #1 Open source multi-media multi-level security systems (to include fostering of commercial and foreign capabilities through international standards)
- #2 Automated all-source correlation system with integrated advanced/artificially intelligent processing and analysis tools (merge functionality of the cia's computer aided tools for the analysis of science & technology with COPERNICUS/MTACCS architecture)
- #3 Information (database) architecture, multi-media in nature (start doing data driven system design)
- #4 National all-source automated intelligence requirements and collection management system (integrate foreign intelligence priorities committee, disciplinary committee priority documents, and JCS intelligence priorities into a single coherent system which provides accountability and auditing capability to determine customer satisfaction)
- #5 Cheap pop-up satellites, all-weather, multi-discipline
- #6 Computer penetration technology across the board
- #7 Virtual reality/multi-media alteration capabilities including truth validation

• Basic investment strategies were recommended by the INTEL Cell:

- #1 Maximize inter-operability with commercial systems and products
- #2 Facilitate/push international standards

FOR OFFICIAL USE ONLY

#3 Use unclassified sources to maximum extent possible, particularly in building Third World encyclopedic database

#4 Plan for and develop capability to automatically sanitize all intelligence to any level of classification (operators in cell expressed very strong desire to "train as we fight" and create data structure now)

#5 Use Integrated Services Digital Network (ISDN) as core of coalition C4I2 approach

● INTEL Cell architecture issues & highlights:

- National Level: shift to an information architecture vice a system architecture; enforce, nurture, and pursue use of commercial and international standards
- Theater Level: include coalition connectivity and classification constraints in architecture
- Tactical Level: establish global multi-media dissemination capability (to any vehicle/man)

● INTEL cell doctrine issues & highlights:

- National Level: establish unclassified alternative databases & products suitable for broad dissemination to unclassified operators and sharing with allies; completely redefine precision targeting database needs and carry out pre-contingency database fill; develop national knowledge warfare concepts & plans; redefine & realign HUMINT to support contingency planning and execution
- Theater Level: develop Low Intensity Conflict Indications & Warnings (I&W) methods and data elements; develop theater doctrine changes integrating new C3I precision targeting methods into campaign planning
- Tactical Level: remove 10M resolution constraint on U.S. commercial imagery; develop media interaction methods and

FOR OFFICIAL USE ONLY

military occupational specialties; develop collection rules of engagement (ROE) for multi-belligerent pre-war situations (i.e. outlining ROE for C3CM in deterrence phase)

• INTEL Cell technology issues & highlights:

- National Level: install open source exploitation capabilities throughout community; develop single national automated data correlation capability (multi-media with time and location tags on all data to facilitate fusion); develop pop-up satellites for contingencies
- Theater Level: pursue "man in space" and "man on site" capabilities
- Tactical Level: develop multi-sensor battle damage assessment tools for near-real-time battle damage assessment from original delivery platform (e.g. improved gun sensors); develop technology enhancers for covert and clandestine HUMINT--sustained SATCOM power, life support systems; develop single advanced workstation

FOR OFFICIAL USE ONLY

C4I2 Highlights from Global War 1991

- Four C4 points made final day were:
 - Existing Joint Strategic Capabilities Plan (JSCAP) does not have the right mix of C4I2 assets, nor enough all-weather capability early on (AF BGen briefed, elaborated by stating that such basic capabilities as AWACS, JSTARS, AVCCC, and RIVET JOINT had to be obtained by special request for any Middle Eastern contingency, were not pre-planned)
 - Telecommunications advances (especially cellular technologies) will make it much more difficult to "black out" the enemy in 2001
 - By 2001 at least 20 nations will have sophisticated imagery and GPS capabilities enabling them to obtain precise pre-conflict targeting data
 - US satellites lacking a space based defense will be increasingly vulnerable
- Although not influential to the game, there were a number of C4 findings developed by the C3I cell and others:
 - Coalition C3 doctrine and capability do not exist, will be major showstoppers in future (note: funding for support to law enforcement against narcotics target is ideal base upon which to build "coalition" C4 capabilities);
 - A civil reserve C3 capability (similar to aircraft and ship programs), and accelerated COTS C4 procurement, are essential to future effectiveness
 - Proliferation of secure SATCOM, improved traffic discipline and procedures, and accelerated development of data compression and fusion techniques, are critical to future effectiveness
 - C3 must train the way it is expected to fight

FOR OFFICIAL USE ONLY

- Pre-conflict protection of key C3 nodes should be a major concern
- Land-based PLRS too constrained, need to move base stations into space (this point is of interest to BGen Sutton, game participant)
- AF Colonel from SPACECOM, when asked for thoughts of possible interest to Marine Corps, provided a paper with detail on four specific C4I2 areas where he felt USMC could gain greater advantage:
 - Residual Communications Satellites. Old satellites degrade piecemeal, and are left with significant residual capabilities. USMC could obtain more capability from one abandoned satellite than it had in all of DESERT STORM/SHIELD.
 - MILSTAR Medium Data Rate (MDR). First launch in 1997, USMC has chance to define to suit.
 - Global Positioning System Receivers. Will be smaller and cheaper, don't let present costs constrain projections of future buys - his impression is that USMC is backing off from GPS for wrong reasons, will be caught short in future, especially when others (e.g. XVIII Airborne) have completely revised their training, equipment, and organization to integrate GPS into every aspect of their warfighting capability.
 - Secondary Imagery Dissemination (SID). Worldwide dedicated dissemination can be achieved at very modest costs through use of Direct Broadcast Video Satellites as well as residual communications satellites.
- A few intelligence "issues" and recommendations were in various working papers or emerged in discussion:
 - Importance of coalitions to warfighting as well as peacetime engagements absolutely requires a well-developed capability for sanitizing, sharing, and disseminating intelligence to allies (including short-term allies and non-governmental organizations)

FOR OFFICIAL USE ONLY

- Importance of intelligence as the trigger for reconstitution of forces cannot be exaggerated (yet there is little support for fencing intelligence so it can provide the advance warning needed)
- Clear concern over lack of warning capability on destabilizing events including non-military trends and occurrences (warning capabilities needed to trigger reconstitution of forces for Third World regional wars do not exist and will take years to build)
- Increased emphasis required on HUMINT, on analysis even if at expense of collection, and on maintenance of databases in non-traditional areas including trade, environment, medical, and demographic
- Absence of joint doctrine on intelligence, particularly as it might refer to coalition operations and support to law enforcement or to non-governmental disaster relief operations, continues to constrain planners

● Marines participating in game added three observations:

- Service needs a commercial C4I2 strategy or gameplan - LANDSAT, for instance, must be understood as both a resource and an enemy asset to be considered by OPSEC planning
- C4I2 needs a reconstitution/pre-positioned stock strategy and must identify needs for 90-180 day periods of multiple crises
- IMINT "cueing" and constraints on dissemination of available imagery of concern

FOR OFFICIAL USE ONLY

Army Technology Base Seminar Wargame II Results

• Summary of Results:

- Next War Will Probably Be a Sensor War. U.S. will not have a monopoly on sensors, must take extraordinary measures to ensure our dispositions and intentions are protected [are we doing enough in concealment and deception concepts, doctrine, & equipment?]
- Long Range Precision Weapons Will Change Our Concepts of Battle. Precision weapons change tactics and operations, could change our concept of offense; players opt for precision targeting in lieu of heavy forces and direct fire weapons.
- New Technologies May Allow Tomorrow's Soldier to "Be More Than You Can Be". Tomorrow's soldiers will be more lethal, not because the weapons are more lethal, but because they can apply them with greater effect. Computer technology will provide the individual soldier with a portable knowledge base, to include language translation, decision support, fire control, position location, and communications. Training and rehearsal systems will allow the soldier to plan and practice missions prior to combat.
- Even in an Era of Enhanced Technology, Many "Old" Problems Will Persist. Operations in urban terrain, minimization of collateral damage, and distinguishing friendly from enemy will continue to tax our capabilities. Weapons of disruption, with "dial-a-strength" [and tightly focused targeting] will be needed.
- Nothing Works If You Cannot Get It There. The loss of overseas bases makes the issue of lift a critical one. Significant forces will never be "light". In addition to ensuring sufficient strategic lift assets are available, the Army must develop computerized load planning, automated routing, and just-

FOR OFFICIAL USE ONLY

in-time ports; design for transportability, self-deployability, and ability to operate from shipboard bases; and design greater capacity for a given weight or size.

- Four enabling technologies for Airland Battle Future (ALBF):
 - Advanced Signal Processing and Computing
 - Low Observables
 - Neuroscience
 - Biotechnology
- C3I Programmatic Implications: "The problem with C3I is not one of low visibility or funding, but the challenge of an overall architecture for sensors, processing, and communications. Such an architecture exists for Division and above, and for individual weapons systems, but the intermediate structure is extremely diffuse. The key to ALBF is the efficient delivery of information, tailored to the recipient, wherever [and whenever] it is needed. Current approaches focus on automating existing manual processes, and linking those processes that have always communicated. ALBF may require the Army to alter this paradigm." [Emphasis added]
- Following systems/capabilities emerged as critical to the Latin American scenario:
 - Sensors (strategic, tactical, personal)
 - Information fusion/distribution
 - Future Soldier System
 - Physiological Preparation
 - Smart Networked Anti-Air/Anti-Vehicle Mines
 - Anti-Tank Helicopter Munitions
 - Long-Range Missiles
- Following systems/capabilities emerged as critical to the Southwest Asia scenario:
 - Tele-Operated Light Missile
 - Multispectral Sensor System
 - Real-Time Battle Management System
 - Light Satellite/Launch Capability
 - Precision Air Drop Systems
 - Future Solider System
 - Air Defense

FOR OFFICIAL USE ONLY

- Improved Deployability
- Following systems/capabilities emerged as critical to the European scenario:
 - Deception and UAV
 - Chemical Protection
 - Exoskeleton
 - Electric Drive Tank and Attack Air Mobility System
 - Strike Space System
 - Real-time-intelligence, coupled with long-range lethal fires, was the weapon of choice
 - Deception units, coupled with smart minefields, gave both the illusion of force and enough lethality to maintain the ruse
 - Ability to forage power from forward locations was important because of the distances involved
 - SOF forces acted as queuing system for space strike system when UAVs could not survive in surface-to-air missile environment

FOR OFFICIAL USE ONLY

Overall Conclusions

- We need to play in these wargames--not only at Navy, but also at Army. We should consider sponsoring our own C4I2 Wargame to discuss and develop new concepts and doctrine for C4I2, and to develop and test new approaches to C4I2 architectures and technologies.
- Cost is not going to be an issue--we need to make the case for C4I2 as a multiplier, and to show how savings in C4 can pay for I2 improvements.
- We need to do much better at providing C4I2 support (not just intelligence, but C2, C4, and Interoperability) to all aspects of the Concept-Based Requirements System (CBRS). It would help if a Concept of Operations for C4I2 Support to CBRS were developed and formally promulgated.
- Marine Corps relationship with Navy and MTACCS management relationships with COPERNICUS appear to be well in hand--we must continue to provide flag-level nurturing of that emerging partnership.
- GPS is going to be a major factor in future information technology architectures--we need a game plan that goes beyond mere acquisition and thoroughly reviews how all of our mission areas will be impacted and how this may change their concepts and doctrine.
- We are extremely vulnerable to C3CM from single brilliant high school hackers, as well as the more obvious organized government organizations. The flip side of reliance on commercial carriers and capabilities is vulnerability to non-governmental threats. This needs more study and emphasis.
- Joint interoperability has finally achieved "cultural acceptance" and is recognized as a requirement across agency and service lines.
- Coalition interoperability and intelligence sharing has not achieved cultural acceptance, and will require study and emphasis.
- Media operations, both exploiting media voice and video, and providing to media that voice and video

FOR OFFICIAL USE ONLY

image we wish to convey to foes and publics, are clearly of great concern to flag personnel and their staff. However, there is no clear appreciation for how we come to grips with the need to have concepts, doctrine, personnel, and perhaps special equipment for this task. One member of the team proposed that the services should widen the intelligence field to encompass all forms of information, and develop media/open source specialists with an established career pattern. Another player commented that today we have low ranking inexperienced personnel on single tours performing "PAO" functions--and generally along baby-sitting lines rather than interaction lines. Would be interesting to host a small Intelligence/PAO/SJA conference to discuss possible concepts and manning requirements.

- The operators in the INTEL Cell (including the Navy O-6 playing the CINC and a Navy O-6 Wing Commander from DESERT STORM) were adamant in their requirement for unclassified information, both for use with our own operators and action officers who do not have anything better than SECRET (if that) and for immediate sharing with coalition partners. They were adamant that we should "train as we intend to fight", and that the data bases and standard families of products should include unclassified products (imagery as well as text) that do not require "in extremis" waivers to disseminate to uncleared personnel. This tracks with FMFLANT's recent expression of requirements for a broad range of unclassified recognition manuals, "how they fight" handbooks, and other data. USMC should keep pushing for change within defense intelligence on this one.
- Besides the application of processing technologies, the one area where new investment in technologies was clearly needed was that of HUMINT support. Precision targeting and related changes in tactics would appear to require significantly improved covert (SOF) and clandestine (non-official cover) HUMINT assets throughout the Third World--they don't have the secure sustainable (battery life) communications they need.
- "Low tech" threats will be amenable to "high tech" targeting only if there are people on the ground able to bring long-range fires on target. Marine Corps may be at risk of losing a significant portion of its deterrence/presence mission to SOF personnel able to

FOR OFFICIAL USE ONLY

"dial-a-missile". We need to think through a range of constabulary/peace-keeping/disaster relief missions and capabilities in the context of precision targeting/ "covert guidance" capabilities.

C⁴I MANAGEMENT CAMPAIGN PLAN: PROPOSED CHANGES IN HOW WE DO BUSINESS

**Robert David Steele
USMC Management Analyst**

16 July 1992

**Resources Management Division
Command, Control, Communications, Computers,
and Intelligence Department
Headquarters, U.S. Marine Corps**

Preface

The campaign plan offered here is founded upon several premises.

With respect to "process", it is assumed that we do not do as much as we should in the area of "command & control"; that we have limited influence over C⁴I resources controlled by other Marine Corps functional managers; and that we have virtually no means of monitoring resource programs outside the Marine Corps, nor of interesting external functional managers in our requirements and capabilities. In short, we are budget driven rather than mission driven, and parochial rather than universal in our planning and programming.

With respect to substance, it is assumed that we have failed to fully define and integrate "intelligence", including information about friendly, neutral, and environmental conditions, into our C² and by extension our C⁴I concepts, doctrine, and architecture, and that we are not adequately influencing Marine Corps concepts, doctrine, weapons & mobility systems acquisition, and training & education.

There are several additional prefatory observations to be made with respect to circumstances within which Marine Air Ground Task Force (MAGTF) command & control must be exercised: trinitarian warfare is no longer the predominant form of conflict; strategy and tactics have merged to an unprecedented extent; the dichotomy between peace and war no longer exists; and civilians--especially policy makers and foreigners--play a role in our operations that was never understood nor envisioned by traditional students of the art of war. It is clear that our campaign plan must be radical in its orientation if it is to address the radical changes in our circumstances and the threats facing our commanders.

*This campaign plan therefore also addresses the role of training and education (T&E) as the "flip side" of C⁴I--in essence, the better our T&E, the less we must communicate and compute, and the more our C² can be implicit and immediate rather than explicit and delayed by technical, organizational, or circumstantial friction and the fog of war. T&E is the foundation for C², just as communications and computers are the instruments of C²; intelligence and information are the sources of energy for the organism as a whole. Although not discussed in detail, references are also made to areas of possible improvement *vis a vis* concepts, doctrine, and acquisition.*

Finally, this campaign plan recommends specific steps toward developing a command & control policy and evaluation process which in turn will increase our influence over all Marine Corps C⁴I resources, and help us to indoctrinate others with our vision of C⁴I.

Introduction

Although C⁴I is defined as command and control, communications, computers, and intelligence, in fact we seem to avoid coming to grips with the theory and practice of command and control (C²), and spend most of our time dealing with the technical and fiscal minutia of communications and computer equipment procurement, and the processing of intelligence which is pushed at us rather than pulled by our individual Marines.¹

The figure below provides an illustration of our C⁴I resource management environment.

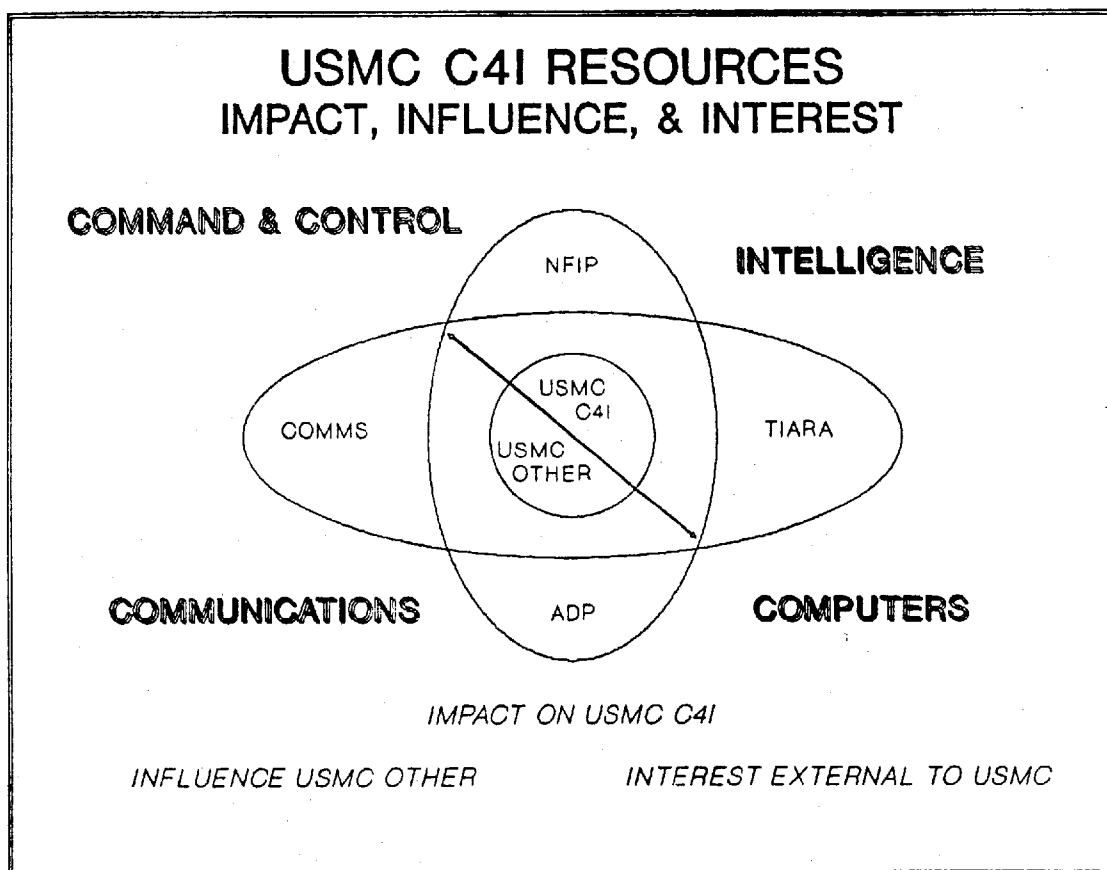


Figure 1. The Marine Corps C⁴I Resources Environment

¹ My thinking on this point has been encouraged by Captains L.R. Kirchner, A.L. Saunders, K.G. Trautman, and J.N. Williams, "C⁴I²: Will It Improve the Marine Corps' Combat Capabilities?" (Paper for the Communications Officers School, 1 May 1989).

The situation is, however, even worse than that depicted, for our consumer--the basic Marine--and our consumer unit--the MAGTF commander and his staff--are not being provided with concepts, doctrine, training, and systems which fully integrate C4I requirements and capabilities. The situation is exacerbated when expanded to include joint and other service concepts, doctrine, training, and systems, all of which could empower but generally constrain our Marines attempting to function in joint and combined operations.

The figure below provides an illustration of our broader C⁴I management environment:

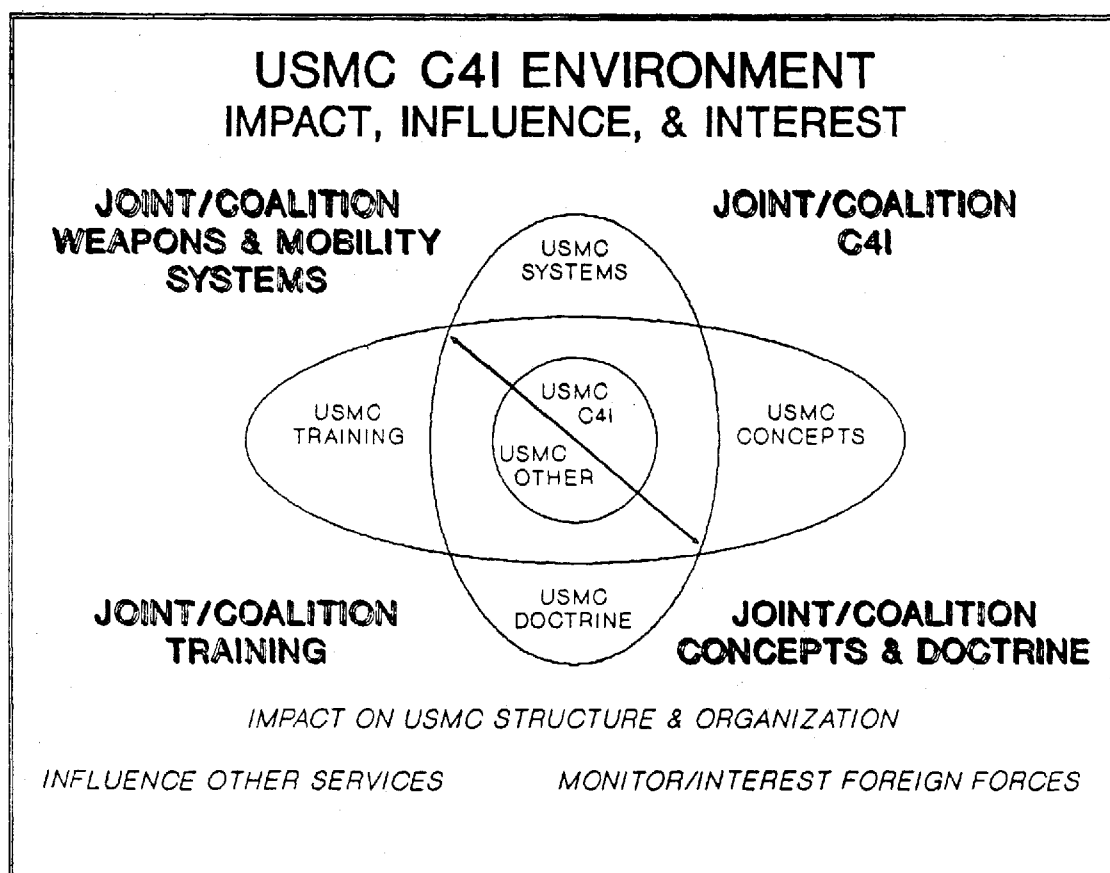


Figure 2. The Marine Corps C⁴I Service Environment

In brief:

-- concepts do not exploit the ability of C⁴I assets to serve as maneuver elements;

-- doctrine does not strike a balance between essential communications and "nice to have" communications;

-- training does not instill knowledge which would allow Marines to forego many communications; and

-- systems--both weapons systems and mobility systems--have been and continue to be acquired without regard to the absence of near-real-time intelligence data or encyclopedic mapping, charting, & geodesy (MC&G) data essential to support the employment of those systems.²

Changing Our Process

In a declining resource environment, complicated by recurring order of magnitude increases in the availability of multi-media information--and commensurate increases in the expectations of our Marine consumers for data, information, and intelligence--we must change the way we do business.

Besides spending too much time playing the budget game, and not enough time establishing and influencing policy, we are also focusing only on those resources which are directly under the purview of the Assistant Chief of Staff (AC/S), C⁴I. Between the delegation of procurement authority to Commanding Generals, and the power of other functional managers in the Marine Corps (e.g. Aviation, Installations & Logistics), we would be hard-pressed to influence, much less impact, on their decisions in the C⁴I arena even if we did have a mechanism for establishing policy, doing integrated (cross-functional) planning, and evaluating our requirements across mission area and command boundaries. Since we do not have such a process, we are restricting ourselves unnecessarily. Beyond the Marine Corps, within the other services, the theaters, and in the civilian community, we have virtually no influence.

Total Quality Leadership (TQL), Corporate Information Management (CIM), and Public Entrepreneurship (PE) all have something to offer our discussion of how to improve our process of enabling and empowering Marine commanders and their staff through the provision of communications, computing, and intelligence & information capabilities. The latter portion of this plan will address the role T&E as the "flip side" of C⁴I; paradigmatic changes in C⁴I must be accompanied by

² The average fast-moving airframe, for instance, has roughly 60-90 minutes of loiter time; the intelligence sensor strings simply do not exist able to provide that weapons system, with its limited loiter time and precision munitions, the near-real-time intelligence necessary to attack "low slow singleton" targets such as are characteristic of the Third World and the expeditionary environment. Worse, as was found in Desert Storm, the precision mapping data is simply not there for the Third World--it took 60 days to obtain the MC&G data necessary for TOMAHAWK and HARPOON targeting; this is the same MC&G data needed for 1:50,000 tactical maps, also not available for most of the Third World. For a detailed review of MC&G shortfalls of concern to the Marine Corps, see USMC Intelligence Center, Overview of Planning and Programming Factors for Expeditionary Operations in the Third World (Marine Corps Combat Development Command, 1991).

corresponding changes in T&E, or they will be irrelevant and ineffective if not counterproductive. Implicit in the latter discussion is the need for a change in the substance of what we communicate and compute.

Total Quality Leadership

Total Quality Leadership³ (TQL) is helpful in that it focuses attention on the "customer", encourages management to empower individual employees, increases attention to long-term commitments and the prevention of problems, and provides a structured process for monitoring and maintaining improvements. TQL does not provide a good means of distinguishing between policy and practice--the C⁴I Department may practice TQL and still abdicate its policy function.

Corporate Information Management

Corporate Information Management⁴ (CIM) is helpful in that it focuses attention on the data foundation for operations, and stresses the importance of identifying and eliminating data redundancies while improving the utility and accessibility of data required by the customer. It merits comment that CIM is at heart an evaluative process, one requiring judgements and decisions about the value of data. CIM requires the elimination of inefficient or ineffective communications pipelines and computer processes.⁵

Public Entrepreneurship

Public Entrepreneurship⁶ (PE), a relatively recent topic in public administration literature, makes a critical distinction between "steering" and "rowing", emphasize the need to manage and evaluate performance based on missions and outcomes instead of resource inputs, and introduces the concept of "retained earnings" as a means of increasing flexibility and innovation in public administration. The principles of PE form an important foundation for this campaign plan. Below, each principle is briefly related to the C⁴I Department

³ A useful and concise summary of TQL principles is provided in the HQMC Bulletin Board; definitions, a process description, and a bibliography are available.

⁴ CIM, as set in motion within the Department of Defense by Paul Strassmann of the Defense Information Systems Agency (DISA).

⁵ One officer has commented that it is important to note that CIM is not an implementation process, and that this constitutes a major policy problem.

⁶ David Osborne and Ted Gaebler, Reinventing Government: How the Entrepreneurial Spirit is Transforming the Public Sector, From Schoolhouse to Statehouse, City Hall to the Pentagon (Addison-Wesley, 1992).

mission and possible changes in how we do business. In general, entrepreneurial organizations:

◆ **Steer more than they row**

This is the most fundamental principle. This principle is about leverage; about reducing the amount of time C4I Department personnel spend pushing paper and administering programs, and increasing the amount of time they serve as catalytic agents, empowering others within the Marine Corps, and influencing others outside the Marine Corps. Consider:

"When governments separate policy management from service delivery, they often find that they have no real policy management capacity."⁷

*"Any attempt to combine governing with 'doing' on a large scale, paralyzes the decision-making capacity. Any attempt to have decision-making organs actually 'do', also means very poor 'doing'."*⁸

"Steering organizations set policy, deliver funds to operational bodies (public and private), and evaluate performance--but they seldom play an operational role themselves. They often cut across traditional boundaries; in fact, their members are sometimes drawn from both the public and private sectors."⁹

There are two points I would stress here: first, that steering is not possible without evaluation--we must be aggressive in establishing a Service-wide capability to evaluate requirements and capabilities. Ideally we should also have means of evaluating C4I requirements and capabilities outside the Marine Corps, not only within the Department of Defense (DoD), but within the civilian agencies of the government and within the private sector. It would be helpful--for instance--to have, for each C4I function and each C4I system (including joint and other service systems) a single one-page "executive evaluation" of that function's health and/or that system's role in Marine Corps C4I, together with a short description of unfunded deficiencies and needed modifications. The "stop-light" charts are

⁷ Osborne and Gaebler, supra note 5, page 39.

⁸ Osborne and Gaebler, supra note 5, page 32, quoting Peter Drucker, The Age of Discontinuity (Harper, 1978), page 233. Italics in original.

⁹ Osborne and Gaebler, supra note 5, page 40.

excellent, light-years ahead of prior management tools in Marine Corps C⁴I, but they don't tell me what specific critical information paths each system is responsible for, nor do I get a good feel for where the choke points are by type of information, originator of information, classification, media, etcetera.¹⁰

The second point follows naturally from the first: there is a role to be played in Marine Corps C⁴I management by private sector personnel, and there is a role to be played in DoD and private sector C⁴I management and development by Marine Corps officers and civilian employees.¹¹ AC/S C⁴I should consider such initiatives as the establishment of an Industrial Advisory Council for Marine Corps C⁴I, and the detailing, association, or regular dispatch of Marines to selected private sector enterprises including such organizations as the Information Industry Association and the Interactive Multimedia Association.¹²

◆ Empower communities rather than simply deliver services

We seem to have agreed that our "customer" is the Marine Air Ground Task Force (MAGTF) commander, and that that customer's identity should be understood to include the MAGTF's role as the nucleus of a Joint Task Force (JTF). What really seems worth exploring here is: how do we define empowerment? My view is that giving the MAGTF commander money and procurement authority in the C⁴I arena is like giving a child matches. It is simply too fast moving an environment for distributed decision-making. Instead, we should focus on giving the MAGTF commander tools, knowledge (education and training) about those tools, and access to data--and most of that data should be

¹⁰ "Structured analysis & design" is the information technician's method for carefully evaluating what data comes into a work unit, the nature of that data, how the data is transformed at each point in the process, where the data resides or is forwarded to, and--to the extent management desires--what impact if any the data has on operational decisions. At the risk of stating the obvious, much of our communicated and computed data is irrelevant to operations and ignored by the consumer the data is intended to serve.

¹¹ There are two aspects of private sector involvement in military C⁴I that must be constantly kept in mind, both representing military dependence on private sector decisions about commercial C⁴I capabilities. In the first instance, as has been amply documented, our reliance on commercial communications for close to 90% of our capability--without a commensurate investment in private sector security and survivability--leaves us vulnerable to interruption of services. At the same time, we have given the private sector little incentive to modernize, building our C⁴I procurements based on hardware costs vice functionality. Cf. Lee Paschall, former Director of Defense Communications Agency, and James Stansberry, former Commander, Air Force Electronic Systems Division, as cited in Thomas P. Coakley (ed.), C³I: Issues of Command and Control (National Defense University, 1991), respectively pages 119 and 206.

¹² Both of these organizations have local headquarters--the first is based in Washington, D.C. and the second in Annapolis, Maryland.

unclassified.¹³ If it is the MAGTF commander's responsibility to shape the battlefield and win battles (including humanitarian assistance battles), then it is our responsibility to shape the MAGTF commander's mind and to give him and his staff the tools they need to command & control. In short, we are not in the communications, computing, or intelligence business. We are in the command & control business.¹⁴

¹³ Regarding consumer demand for unclassified information, it merits comment that the Marine operators, Warfighting Center action officers, and acquisition project managers whom I knew when I served as the Special Assistant and Deputy Director of the USMC Intelligence Center insisted on the utility of unclassified information for their daily endeavors. At a more formal level, as documented in the C4I trip report on "Technology Initiative Game - 1991", the number one intelligence priority identified to the flag panel was improved open source exploitation. The report was disseminated informally to C4I principals throughout the Marine Corps after approval in AC/S C4I² Ltr C4I2R dtd 3 Jan 92. It is important to note that many professionals share the view that too much information is classified for the wrong reasons; I personally believe the Marine Corps should be a strong advocate of "no classification without justification". Consider the following quotation:

"Everybody who's a real practitioner, and I'm sure you're not all naive in this regard, realizes that there are two uses to which security classification is put: the legitimate desire to protect secrets, and protection of bureaucratic turf. As a practitioner of the real world, it's about 90 bureaucratic turf; 10 legitimate protection of secrets as far as I'm concerned."

Above by Rodley B. McDaniel, then Executive Secretary, National Security Council and former Senior Director, (White House) Crisis Management Center, in Coakley, supra note 10, page 68.

-- Several additional themes related to consumer satisfaction must be considered: first, recognizing that consumers by definition believe they are pressed for time, communications to the consumers must be "high-burst" and tailored to get the consumer to understand the information and focus on the need for action--this is--by one account--the reason television and multi-media are such powerful communications tools; second, the information which is provided to the consumer must be responsive to their needs. This includes a requirement to fully integrate the C4I manager into the operational process; to empower the consumer so they feel comfortable pulling information from the array of systems and databases available to them; and creating a C4I infrastructure which includes forward-looking analysis and the ability to identify and then push some information to the consumer when appropriate. Cf. various national authorities cited in Coakley, supra note 10, pages 47-48, 50, 296, 299.

¹⁴ In the "old Corps", it was "shoot, move, and communicate". Now it is fashionable to speak of the "OODA Loop" (orient, observe, decide, act). Both refer to functional command & control capabilities, rather than technical measures. We must be very cautious about getting caught up in technical and quantitative performance measures. More the point, we should refocus on who our customers are, what they want, and whether or not they are happy. However, while customer satisfaction may be the ultimate measure of our success, if our customer is an uninformed customer, unfamiliar with the costs and trade-offs of C4I, unfamiliar with the impact of changing technology on how information can be presented, then customer satisfaction will be a hollow

◆ **Encourage competition rather than monopoly**

Privatization of effort, and consideration of alternatives developed by others (e.g. the other services), are means of improving our return on investment. However, while competition is to be encouraged in the provision of services to the MAGTF commander and supporting entities, governance--policy-making and related steering functions--should not be delegated. AC/S C⁴I may wish to review how the C⁴I deputy program managers and their staffs within the Marine Corps Systems Command (MARCORSYSCOM) spend their time. Are they primarily Contracting Officer's Technical Representatives (COTR), "captured" by a specific system and its prime contractor, or are they focused on broader functional requirements, and brokering solutions--in partnership with customers--that are not hostage to individual systems? Are the action officers within the C⁴I Department at HQMC primarily file clerks and recording secretaries, or are they catalysts and innovators, agents of change in and out of the Marine Corps?

◆ **Are driven by their missions, not their rules**

My perception of the bundle of regulations and processes that comprise the Marine Corps C⁴I "system" is that we are over-loaded with "requirements" and have a kludge of competing and counter-productive communications and computing capabilities spread across functional and organizational boundaries.

"...we too often develop our communications requirements by listing all nets called for by doctrine, without adequately analyzing what specific communications requirements will be for a given operation...doctrinal nets are too numerous to be supported."

"C⁴ Division, HQMC should...provide policy guidance on C² issues...and not allow themselves to be preoccupied with hardware acquisition."¹⁵

victory. First we must educate, then we must evaluate need, and only then can we truly set about the task of establishing a Corps of satisfied customers.

¹⁵ Kirchner, Saunders, Trautman, and Williams, supra note 1, page 5-23. Charles Snodgrass, Vice-President of Electronic Data Systems Corporation and former Assistant Secretary of the Air Force for Financial Management, has stated "...we buy computers in ways that make no sense. ... We essentially buy computers on the basis of hardware cost when, in the current systems, hardware is about 20 per cent of the cost and software is about 80 per cent. Yet, for historical legislative reasons [the Brooks Act], we let that 20 per cent tail drive the 80 per cent dog. I think many of the failures you see in government command and control, communications, and computer acquisition are directly related to the Brooks Act." Croakley, supra note 10, page 189. This

The results of the Technology Initiatives Wargame 1-91, and the demands of the operators for predominantly unclassified information dissemination systems and unclassified intelligence products, merit recurring reflection by AC/S C⁴I and his Colonels.¹⁶ The requirements of the operators for unclassified products should not lead to an abdication of our responsibility in the information security arena. What operators really mean, when they say unclassified information, is "hassle-free" information. We must continue to move toward full encryption of all tactical communications in order to deny our increasingly sophisticated Third World opponents any window into our operations.¹⁷

thought process can be naturally extended by inquiring if, instead of software driving the acquisition, a fundamental review of what and how the customer wants to see information should drive acquisition. As Paul Strassman has stated, too many people automate hard-copy processes (e.g. digitally transmit every message to every person) rather than going back to basics and rethinking the process in its entirety. Paul Strassman, Information PayOff: The Transformation of Work in the Electronic Age (Free Press, 1985), pages 116-135 passim.

¹⁶ The Marine Corps invested an SES, six Colonels, two Lieutenant Colonels, and a GS-14 in this effort, resulting in a comprehensive trip report with a great deal of substance, supra note 12. Among the executive highlights:

- Technology is not the showstopper--management is where we must change the way we do business.
- Architecturally we must define a completely new paradigm of what information we need, how we handle it, and how it is delivered to the user; this new paradigm must include an information architecture (vice a system/command architecture) approach, must extend to include commercial and coalition capabilities, and must integrate Global Positioning System (GPS) data.
- Doctrinally we need to ensure we are represented in joint and other service "doctrine" forums. Cost will not be an impediment to progress--lack of innovative management at all levels is the show-stopper. We need a new approach to C⁴I², both as functional mission area and as a new and powerful form of warfare. While some might not agree, many would suggest our new concepts must integrate unanticipated short-term coalitions, media operations, C4I2 oversight over weapons system design and employment concepts, new data requirements associated with precision targeting, unclassified data requirements necessary for real-time and coalition operations, and a very broad understanding of needed developments in concealment, deception, and covert communications capabilities suited to future adversarial C⁴I² capabilities.

¹⁷ Raymond Tate, former Deputy Assistant Secretary of the Navy and Deputy Director, National Security Agency, has stated: "...in the *Mayaguez* case, ... while the President had command and control, the enemy knew everything he was going to do at about the same time as the commanders on the site, and took some direct actions against them. ... The forces that transmitted the orders were using HF voice, all in the clear. Orders to the helicopters to take the islands were passed from the Air Force to the Navy. Over the circuit the two commanders revealed how many helicopters and how many men were involved, where they were going, at what

◆ Fund outcomes rather than inputs

"Public entrepreneurs know that when institutions are funded according to inputs [fair share budgets], they have little reason to strive for better performance. But when they are funded according to outcomes, they become obsessive about performance."¹⁸

Do we know the quantity, quality, and cost of every C⁴I service we provide to the MAGTF commander, the MAGTF staff, and members of the supporting establishment? What are our performance indicators? How do we tell success from failure vis a vis command & control, communications, computers, and intelligence? Is the volume, format, and readability of our message traffic part of the solution or part of the problem? Have we lost sight of where intelligence fits in the over-all scheme of information needed by the commander and his staff? To what extent have we empowered the MAGTF commander and his staff to increase, decrease, modify, or reroute different types of information in different media and format?

"If you can't reward success, you're probably rewarding failure...rewarding failure creates bizarre incentives. It encourages (individuals) to accept the status quo. It encourages (individuals) to ignore the root causes (of the problem) and simply to chase (symptoms)."¹⁹

If we were to manage for performance, applying TQL principles, we would avoid the mistakes of many organizations which apply TQL in form but not in substance.

"In practice, however, most of these organizations implement only a part of the Deming approach. Many fail to track the results of their work, for instance, or to define exactly what results constitute quality performance. Very few focus on the basic systems that drive their organizations, so they remain in the realm of 15 percent solutions, rather than transforming their

time, and the replenishment rate." Raymond Tate, cited in Coakley, supra note 10, page 10. Emphasis in the original.

¹⁸ Osborne and Gaebler, supra note 5, page 139. Brackets added.

¹⁹ Osborne and Gaebler, supra note 5, page 149.

organizations."²⁰

A cautionary note must be sounded here: TQL "mechanics" can rapidly achieve a momentum of their own in which a great deal of time is spent in cheerleading and measuring, and no time is spent in talking to the customer and working with the customer to achieve ad hoc solutions that are effective without necessarily being elegant or technically "perfect". The customer is the "first system" with which all other systems must be inter-operable.²¹

The POM & Fiscal Branch of the Resources Management Division, with one additional person, has great potential as a vehicle for the transformation of C⁴I in the Marine Corps.

"...in government, the most important lever--the system that drives behavior most powerfully--is the budget. Most managers work in government, after all, not to enrich themselves but to have some positive impact on their community. That opportunity is available only to the degree that they get control over resources. How do they get that control? Through the budget system. Results-oriented organizations find that they ultimately need to develop budget systems that fund outcomes

²⁰ Osborne and Gaebler, supra note 5, page 160. An example of a 15% solution is the move of message traffic from hard-copy to terminal delivery. An example of an 85% "core" solution is to provide every Marine with electronic connectivity to every other Marine, and access to topical files in each mission area across organizational boundaries and external to the Marine Corps.

²¹ Strassmann has refined techniques for actually valuing information from different sources, establishing the degree to which they do or do not contribute to the consumer's productivity (mission accomplishment). Cf. Strassman, supra note 14, pages 136-150. To my knowledge no one has ever attempted to evaluate the "value" of information destined for (but not necessarily delivered to, read, or exploited by) the MAGTF commander and his staff. The whole area of C⁴I policy interaction with consumers needs to be scrutinized. Among comments made: Richard Stilwell (Chairman, DoD Security Review Committee): need to plan for information implications of crisis versus peacetime, transition to war, eliminate products and wait for consumers to define new or continuing demands; Lionel Olmer (former Undersecretary for International Trade in the Department of Commerce): "it isn't enough merely to be accurate and sometimes it's not even enough to be timely. There are several other characteristics that have to go along with accuracy and timeliness, the most important of which is relevance. ... You've got to be part of the (operational) process. There's no other alternative."; Mark Lowenthal, Acting Director, Office of Strategic Forces Analysis, Bureau of Intelligence and Research, Department of State: "The mistake, I think, that consumers make in the Executive is that they probably believe that everything else is being covered and waiting to be tapped." (i.e. consumers do not realize that gaps exist, and have not been forced to decide trade-off issues.). All citations from Coakley, supra note 10, respectively pages 336, 340, and 346.

rather than inputs."²²

The "capabilities sets" approach to C⁴I programming and budgeting is a brilliant intermediary strategy that is already paying dividends in terms of increased support for unfunded C⁴I deficiencies. However, as I review that material, I ask myself four questions:

- How does this all fit together?
- What are the units of measure?
- What does it cost us in non-fiscal terms?
- What is missing from this picture?

In general, I think we have a long way to go in planning for the complete integration of C⁴I hardware, operating systems, and software. We are allowing individual electronic units of measure (an ELINT signal, a text message) to dominate our planning, while avoiding the harder issues of hard-copy conversion and multi-media fused data presentation. I also think that we have avoided coming to grips with the totality of space, weight, and training costs imposed on us by the multiplicity of C⁴I systems. Finally, I am not comfortable with either our information security posture, nor our doctrine. With whom should any Marine be able to communicate with? How do we put the full power of the Nation, the theater, our allies, and the MAGTF behind that single Marine on point?

◆ **Meet the needs of the customer, not the bureaucracy**

Although we have chosen to focus on the MAGTF/JTF commander as our customer, this should be regarded as an intermediate step in our restructuring and reorientation process. Ultimately, our customer is the individual Marine. There are remarkable similarities between the TQL emphasis on empowering the individual employee, and Field Marshall Rommel's emphasis on recon pull, where the Corporal on point, quite literally, was "in charge" of the company, battalion, and division behind him.

When was the last time anyone representing AC/S C⁴I asked any Marine what they thought about our C⁴I capabilities? Customer-driven systems increase accountability and responsiveness, stimulate innovation, provide choices of interest to the customer, waste less by matching supply to demand, and empower customers.

²² Osborne and Gaebler, supra note 5, page 161, emphasis added. The authors distinguish between "outputs" (quantities), and "outcomes" (qualities).

"There is simply no substitute for direct access...it keeps managers informed, it keeps them in touch, it keeps them honest."²³

The figure below itemizes a number of different means by which our Marines could impact on C⁴I capabilities planning and programming.²⁴

- | | |
|----------------------------|-----------------------------|
| ◆ Customer Surveys | ◆ Customer Service Training |
| ◆ Customer Follow-Up | ◆ Test Marketing |
| ◆ Community Surveys | ◆ Quality Guarantees |
| ◆ Customer Contact | ◆ Inspectors |
| ◆ Customer Contact Reports | ◆ Ombudsmen |
| ◆ Customer Councils | ◆ Complaint Tracking System |
| ◆ Focus Groups | ◆ 800 Numbers |
| ◆ Customer Interviews | ◆ Suggestion Boxes |
| ◆ Electronic Mail | |

Figure 3. Listening to the Customer

Using only myself as an example, when I have to communicate with another Marine who is not in the local area my choices are, in order of priority:

- ◆ Electronic Mail
- ◆ Facsimile
- ◆ Telephone
- ◆ Correspondence
- ◆ Message

It takes me up to a month to get a message out of this Headquarters, in part because I don't have message drafting capabilities on my work station, and in part because optical character recognition and message format add two other levels of potential error and return. Correspondence, with staffing and releasing, takes about a week. Telephone, in the absence of voice mail on the other end, can take several days. Facsimile and electronic mail, on the other hand, are "send and forget/what you see is what they see" capabilities.

We have much to gain, and nothing to lose, by undertaking a comprehensive survey of what our individual Marines, at every level of command and staff, within the Headquarters, the Fleet Marine Force, and the Supporting Establishment, would

²³ Osborne and Gaebler, supra note 5, page 170.

²⁴ Osborne and Gaebler, supra note 5, pages 177-179, where additional detail on each method is provided.

like to have in the way of C⁴I capabilities (to include unclassified reference information).

◆ Concentrate on earning, not just spending

"Our (government) budget systems drive people to spend money, not make it. And our employees oblige. We have 15 million trained spenders in American government, but few people...even think about revenues. No one thinks about profits. The typical public employee, in fact, resents that he or she occasionally has to worry about revenues--because budgets falls short or taxpayers revolt. ...most believe they are doing God's work, and the public should be grateful. ...can you imagine the creativity they would turn loose if they thought as much about how to make money as they do about how to spend it?"²⁵

There are a number of ways to generate revenue apart from the established allocation process. Money can be raised by charging fees (either to the public for a service rendered with capabilities that are surplus in peacetime, or to the Marine user as a means of highlighting service cost). Besides raising funds, user fees lower demand and identify the priority users who really value the services provided. Exercising a "return on investment" perspective on spending helps increase long-term revenues by reducing or eliminating expenditures that are not competitive. Allowing subordinate managers to retain savings sparks innovation by making "seed capital" available at all levels of the organization; it also provides a source of very flexible contingency funding that is responsible to the short-term needs of the subordinate manager.

Changes in the budget process would have to be negotiated with the Comptroller, but there is reason to hope for success: Robert Stone, Deputy Assistant Secretary of Defense for Installations, has adopted many of these ideas and applied them to great effect.²⁶ Pending any major changes in the budget system, one interim approach might be the establishment of a C⁴I "loan pool"

²⁵ Osborne and Gaebler, supra note 5, pages 195-196.

²⁶ Osborne and Gaebler, supra note 5, pages 8-9, additional references throughout the book. It will not be easy. "...budgets drive policy in this government; policy does not drive budgets. ... I haven't got enough fingers and toes to count for you the number of Presidential Directives that really don't have very strong teeth because the OMB budget examiner managed to make sure there was no money to support the effort." Robert Rosenberg, Policy Assistant to the President for National Security Affairs, as cited in Coakley, supra note 10, page 117.

against which C⁴I Colonels could draw up to a certain limit. At the same time, we must make all C⁴I personnel "revenue conscious".

"If we want public employees to become 'revenue conscious', we need incentives to encourage them to make money as well as to spend it. Guaranteed incomes create all the wrong incentives. A manager with a hefty budget will act much like a teenager with a hefty allowance. Neither will beat the bushes for new ways to earn or save money."²⁷

The starting point for earnings is found in identifying the true cost of services.

"...most governments have no idea how much it costs to deliver the services they offer. Even if they can give you a budget figure for each service, it typically excluded 'indirect costs' such as administrative overhead, capital costs, and employee fringe benefits. One study of 68 cities found their true costs to be 30 percent higher than their budgeted costs."²⁸

While beyond the scope of this paper, it merits comment that we probably have no means--at the Service or Fleet Marine Force level--of calculating the true cost of each of our mission areas and their inherent systems, no means of establishing the frequency of use (e.g. of tanks on deployment), and therefore no basis for evaluating the return on investment by mission area.

"An enterprising government exposes its subsidies to public light, relies on public pressure to do away with them--and then finds ways to make money from the services involved."²⁹

²⁷ Osborne and Gaebler, supra note 5, pages 212-213. The whole issue of "profit" in government (or "retained earnings") is a contentious one; many members of Congress and their staffs have an ingrained perception that it is inappropriate for a government entity to make a "profit" on a provided service, even if this reduces tax costs.

²⁸ Osborne and Gaebler, supra note 5, pages 216-217.

²⁹ Osborne and Gaebler, supra note 5, page 218. How would a MAGTF commander's requirements change if he knew he could have twenty unclassified facsimile machines instead of a single classified circuit? Or one hundred PC's with encrypted E-Mail instead of an imagery processor?

◆ Invest in prevention, rather than cure

"There was a time when our government focused more on prevention... But as they developed more capacity to deliver services, their attention shifted. ... The bureaucratic model brought with it a preoccupation with service delivery--with rowing. And organizations that focus their best energies on rowing rarely do much steering. They develop tunnel vision."³⁰

What would it mean to the Marine Corps if we undertook a comprehensive review of doctrine, training, and systems, all with the intent of significantly reducing the volume and frequency of message traffic? This sounds remarkably like the COPERNICUS concept which the Navy is rapidly developing into a joint doctrine and acquisition strategy for C⁴I.

Preventive or anticipatory government focuses on solving problems rather than delivering services. By attacking problems in a pro-active fashion, this kind of government provides for both cost-avoidance (not having to pay for the problem over the long run) and cost-reduction (limiting expenditures on services that would not be demanded if they were not offered).

Anticipatory government must engage in strategic planning. Strategic planning is consonant with the Marine Corps' mission-type order perspective.

"At its best, however, strategic planning permeates the culture of an organization, creating an almost intuitive sense of where it is going and what is important. ... In an anticipatory organization, members will work toward where they think the organization will be. 'It is strategic thinking and acting that are important', (says one commentator), 'not strategic planning'. "³¹

By combining strategic planning with mission-oriented budgeting, it is possible to improve cross-departmental "looks" and better anticipate C⁴I costs of decisions in other departments.³² Adding to this a method of tracking the current

³⁰ Osborne and Gaebler, supra note 5, pages 219-220.

³¹ Osborne and Gaebler, supra note 5, page 234.

³² Many observers of the U.S. government recognize an inherent antipathy to strategic planning and integrated analysis. No program can succeed which does not integrate, in addition to "the threat", a sound understanding of friendly capabilities, the domestic political implications of the

value and state of repair of existing systems improves perspective.

*"At all levels of government, accounting records almost entirely ignore what assets are owned, their state of repair, and their value. These systems therefore imply that it costs nothing to use these existing assets. Indeed, they suggest the opposite: by cataloging the costs of maintenance as a current expense, they make it seem cheaper to use up assets than to keep them in good repair."*³³

◆ Decentralize authority

What we are really talking about here is not the decentralization of authority over C⁴I systems procurement, but rather a change in the total Marine Corps organization and way of doing business such that C⁴I changes its nature.

What happens when training & education (T&E) are automated, distributed, and available on-demand (i.e. in real time where necessary), when T&E become the primary means of exerting command & control over the Marine Corps, rather than a side-step from "real" work?³⁴

proposed program, and the bureaucratic realities (e.g. the position of the Office of Management and Budget). For comments along these lines, see discussion by Richard Beal, then Special Assistant to the President for National Security Affairs, among others, in Coakley, supra note 10, pages 23-103 and especially page 30.

³³ Osborne and Gaebler, supra note 5, page 244, italics in the original.

³⁴ Improved T&E, a passion of the former Commandant, General Alfred M. Gray, is totally consistent with General Gray's emphasis on "commander's intent. General Gray is cited admiringly by Richard Beal, who at the time was Senior Director for Crisis Management and Systems in the National Security Council:

- "...what I call Gray's Principle. Gray is a Marine General, commanding officer of Camp Lejeune, and a remarkable man in many respects.
- "General Gray and I were going over some of the concepts that the Navy and the Marines were going to use (in Lebanon), and I asked him, 'How do you keep all this coordinated?'
- "And what General Gray said to me I found very interesting: that in times of stress, every echelon in the organization must understand the organization's immediate goals and act to fulfill them, without further information."

This suggests three changes in C⁴I:

- Significant increase in video-teleconferencing and its related bandwidth requirements;
- Potential reduction in record traffic pertaining to permissions and statuses;
- Potential realignment or merging of T&E funds with those of C⁴I, to create a command & control structure which sees T&E as the integral flip side of C⁴I

The following three passages provide a glance at the heart of why we need to change both C⁴I and T&E doctrine in the Marine Corps:³⁵

"Harlan Cleveland, former dean of the Humphrey Institute at the University of Minnesota (and former senior Federal official), wrote a fascinating book about managing in the knowledge economy called The Knowledge Executive. "In the old days when only a few people were well educated and 'in the know', leadership of the uninformed was likely to be organized in vertical structures of command and control," he said. "Leadership of the informed is different: it results in the necessary actions only if exercised by persuasion, bringing into consultation those who are going to have to do something to make the decision work." Authority, in other words, is increasingly "delegated upward". Collegial not command structures become the more natural basis for organization. Not "command and control" but "conferring and networking" become the mandatory modes for getting things done." Cleveland called this the "twilight of hierarchy".

"While the rest of society has rushed headlong away from hierarchy...most governments have held tight to the reins. Their message to employees has not

As cited in Coakley, supra note 10, page 32.

³⁵ Osborne and Gaebler, supra note 5, pages 253-254, citing Harlan Cleveland, The Knowledge Executive (Dutton, 1985), no page given; and Gifford Pinchot, Intrapreneuring (Harper & Row, 1985), page 304.

changed: Follow orders. Don't use your heads, don't think for yourself, don't take independent action. ... Never, ever, take a risk. (Emphasis added)

"This message is enormously destructive. For decades it has cowed public employees, left the docile, passive, and bitter. ...

"The resulting inertia carries an enormous price tag. "Seeing the waste, some call for more centralized controls," says Gifford Pinchot III. "But the waste is not being created by inadequate controls. It is being created by removing the sense and fact of control from the only people close enough to the problem to do something about it" (emphasis added)."³⁶

One can make the point that we cannot have a workable investment strategy for C⁴I unless we have a matching and complementary strategy for T&E--one without the other will be dysfunctional.

At the same time, the degree to which C⁴I Marines are trained and educated will have an impact on the workability of the investment strategy and the impact of C⁴I on the Marine Corps as well as external organizations.³⁷

- ◆ Solve problems by leveraging the marketplace, rather than simply creating public programs.

In a declining fiscal environment we are naturally required to reduce services, and often prevented from recapitalizing old equipment, retraining people, or modernizing our methods. Besides looking for innovative ways of reducing costs and increasing revenue, the best way we can increase capabilities is by leveraging the efforts of others, not only in the government but in the private

³⁶ One officer has pointed out that in the era of the "gold collar" worker, it is not only foolish to reduce the influence of the knowledgeable employee on day to day processes, but it is also likely to result in more and more calls to the various national, defense, and public media "hotlines" established to detect fraud, waste, and abuse. Today's employee is both intelligent and independent, less likely to be over-awed by authority, and more likely to "blow the whistle" than at any previous time in the history of defense procurement.

³⁷ Osborne and Gaebler, supra note 5, page 275, point out that the federal government spends approximately 1% of the civilian non-postal payroll on training, compared to 3% for Fortune 500 companies. In an environment that is characterized by declining manpower, expanding knowledge, and rapid change, one could make the case that both T&E, and "tools for thought", should be candidates for substantial increases in their share of any organization's budget.

sector.

"The trouble with government by program" is summarized below.³⁸

- ◆ Driven by constituencies, not customers
- ◆ Driven by politics, not policy
- ◆ Create "turf", which are then defended at all costs
- ◆ Tend to create fragmented delivery systems
- ◆ Not self-correcting
- ◆ Rarely die
- ◆ Rarely achieve scale necessary to make major impact
- ◆ Use commands, not incentives

Figure 4. "The Trouble With Programs"

Leveraging the marketplace requires smart informed employees able to monitor and influence the activities of others. Institutionally, there are several strategies which can be pursued:³⁹

- ◆ Setting the rules of the marketplace
- ◆ Providing information to consumers
- ◆ Creating or augmenting demand
- ◆ Catalyzing private sector suppliers
- ◆ Creating market institutions to fill gaps
- ◆ Catalyzing the formation of new market sectors
- ◆ Sharing the risk with the private sector
- ◆ Changing public investment policy
- ◆ Acting as a broker for buyers and sellers
- ◆ Pricing activities through the tax code
- ◆ Pricing activities through impact fees
- ◆ Managing demand through user fees
- ◆ Building community

Figure 5. Strategies for Leveraging the Marketplace

³⁸ Osborne and Gaebler, supra note 5, pages 285-289, where additional detail is provided.

³⁹ Osborne and Gaebler, supra note 5, pages 290-298. See also Appendix A of the book, "Alternative Service Delivery Options", pages 332-348, for additional suggestions. The absence of smart employees with the right level of professional skills in acquisition is a major obstacle to smart C⁴I management. Cf. comments by James Osborne, former Senior Vice President, E-Systems, Inc., in which the ability of government acquisition managers to identify real needs, provide adequate specifications, and establish consensus on their C⁴I baseline is called into question. Coakley, supra note 10, pages 174-176, 180.

C⁴I Campaign Plan: Basic Goals

The actual establishment of goals, objectives, and performance indicators needed to implement a mission-driven budget should be the first step of the campaign. Such an effort could begin with dissemination of this paper, however finally refined through review, together with a survey form aimed at MAGTF commanders and staff.

- ◆ Understand our customers' requirements
- ◆ Understand actual costs of C⁴I services
- ◆ Inform our customers about C⁴I options

Figure 6. Basic C⁴I Goals

One of our first goals should be to understand our customers' requirements in a non-technical high-level context.

Another goal should be to understand the actual cost of our existing and projected C⁴I services.

A third goal could be that of communicating to our customers, in the context of their expressed requirements, some alternative means of achieving their C⁴I goals.

C⁴I Campaign Plan: First Steps

Among early "TQL" steps AC/S C⁴I may wish to consider:

- _____ Establish a C⁴I Policy Coordinator, ideally within the Resources Management Division.
- _____ Establish a C⁴I Policy Group consisting of no more than ten individuals, and hold a one day session focused on policy issues rather than technical or funding issues.
- _____ Establish a C⁴I Resource Council consisting of a representative responsible for monitoring, or representing, each of the "pots" of money which we are actively or peripherally responsible for; sponsor quarterly meetings which present the different programs in terms of

capabilities vice numbers.⁴⁰

- _____ Establish a C⁴I Industrial Advisory Council consisting of no more than ten individuals, and hold a one day session focused on multi-media trends and industry views of needed policy changes within DoD.
- _____ Dedicate one individual to "thinking about the future" and service as a "gatekeeper" for the policy group, the industrial advisory council, and other "steering" mechanisms.
- _____ Conduct a zero-based review of all external representational assignments (committees, working groups), in conjunction with a commitment to increased manning of joint billets and a review of possible industrial liaison opportunities.
- _____ Request National Defense University/Harvard University assistance in conducting a one day command & control seminar in which "lessons learned" from past Executive Program sessions are distilled and presented to C⁴I division and branch leadership.⁴¹
- _____ Prepare an ALMAR which restates our mission in terms of enabling command & control, and charges all MAGTF commanders and supporting establishment commanders with reviewing their C⁴I and their T&E requirements in that light, soliciting suggestions for innovation.

⁴⁰ Within the Intelligence Division alone, apart from the General Defense Intelligence Program (GDIP) and the Tactical Intelligence and Related Activities (TIARA) account, there are individuals who monitor Special Air Force, the Consolidated Cryptologic Program, the Foreign Counterintelligence Program, and--to a limited extent, the Central Intelligence Agency Program. We should charge these individuals with preparing quarterly one-page reports on their respective resource programs, together with a one-page "Marine Corps Strategy" for influencing or leveraging capabilities which exist in those programs. In the communications and computer arena, we should have, in addition to our primary action officer for each, representatives from other major HQMC departments.

⁴¹ Dr. Thomas A. Julian, Director of the Command & Control Research Program, Institute for National Strategic Studies, National Defense University, has something to offer against this requirement. I have previously provided to AC/S C⁴I and C⁴ front office copies of a book summarizing numerous Harvard seminars for U.S. government officials: Thomas P. Coakley (ed.), C³I: Issues of Command and Control (National Defense University, 1991).

- _____ Request Commander, MARCORSYSCOM concurrence and direct USMC Management Analyst to interview C⁴I Deputy Program Managers and selected Project Managers to evaluate the degree to which they feel trapped versus empowered, and their views on what changes might increase their ability to leverage the marketplace.
- _____ Direct USMC Management Analyst to interview selected HQMC C⁴I action officers to evaluate the degree to which they feel trapped versus empowered, and their views on what changes might increase their ability to support a policy steering process instead of a technical acquisition process.
- _____ Discuss with C⁴I principals the best means of arriving at a short (ten page) summary of what various C⁴I services "cost" per unit of measurement; direct the conduct of such a study, to include comparison with other services and private sector.
- _____ Modify mission and tasks of all elements of the Resources Management Division, and some elements of other divisions, to emphasize additional duties in area of program evaluation (including external programs), as well as responsibility for identifying opportunities to leverage external government and private sector programs.
- _____ Identify a field grade officer or civilian (could be GDIP-funded) to augment POM & Fiscal Branch with a view to developing and staffing an internal Marine Corps campaign plan for leveraging and influencing C⁴I monies controlled by other Marine Corps functional managers and general officers.
- _____ Task POM & Fiscal Branch, possibly with the assistance of specialists from the Defense Intelligence College, the Intelligence Program Support Group, and the Comptroller, with developing a concise (no more than ten pages) proposal for implementing an outcome-oriented C⁴I budget process.
- _____ Identify promising Post Graduate School attendees and commission a thesis, perhaps by a team of officers representing each C⁴I military occupational specialty,

which designs, conducts, and reports on a Service-wide survey of randomly chosen Marines and their views on C⁴I deficiencies and requirements.

- _____ Establish an 800 number or an E-Mail address (Department mailbox) to which any Marine may send a C⁴I suggestion, complaint, or observation; require a monthly summary of results.
- _____ Offer the C⁴I Colonels throughout the Marine Corps a firm deal: they will keep any savings they find in their budgets--then charge them with finding better ways of doing business.
- _____ Establish a C⁴I Productivity Enhancement Program to screen and support modest initiatives suggested by individual Marines--use \$200K annually from USMC Intelligence Center budget as seed money, persuade the Comptroller to match with like amount.
- _____ Bring C⁴I project managers from the Warfighting Center (concepts, requirements, and doctrine action officers) for a one-day off-site to discuss emerging concepts in C⁴I and to develop a C⁴I campaign plan tailored to Warfighting Center mission.
- _____ Integrate the strategic planning efforts of the C⁴I Department and the Training & Education Center. Through the T&E Branch of the Resources Management Division, establish a small joint working group with HQMC and MCCDC T&E representatives to examine the implications of multi-media and video-teleconferencing for both C⁴I and T&E; charge this group with providing a brief (ten page) tour of the horizon and possible course of action intended to enhance T&E through the application of innovative C⁴I, while striving to reduce C⁴I costs through substitution of T&E enhanced self-sufficiency requiring less C⁴I support.
- _____ Discuss with C⁴I principals, and with Comptroller if appropriate, how we value our existing C⁴I assets, and whether any change to this methodology would be beneficial to our understanding and practices.

_____ Develop a C⁴I media campaign to inform others of Marine Corps interests and doctrinal & technical directions.⁴²

Conclusion

Over-all, this campaign plan seeks to:

- ◆ isolate and emphasize a C⁴I policy-forcing capability that is "visible";
- ◆ better integrate our efforts with those of the private sector;
- ◆ deliberately nurture a "future" oriented staff capability;
- ◆ sponsor more attention to "command and control" as the predominant mission, function, and objective for the C⁴I community in the Marine Corps;
- ◆ educate our consumers about C⁴I capabilities and establish a symbiotic relationship with our T&E counterparts--with the objective of radically altering concepts, doctrine, and acquisition priorities in other mission areas;
- ◆ develop an institutional and integrated (cross-program, cross-function) C⁴I program evaluation capability;
- ◆ alter the manner in which we approach our Service and subordinate command C⁴I budgeting process--focusing on desired outcomes instead of available inputs; and finally, to
- ◆ methodically consider how best to influence C⁴I actors external to the Marine Corps, and--through appropriate public affairs efforts directly related to our Congressional

⁴² The existing mission and tasks of the Resources Management Division, and the POM & Fiscal Branch in particular, include explicit provision for handling the C⁴I Public Affairs function. It was my view, accepted by the Director of the Division, that POM inputs, Congressional testimony, and public presentations (speeches as well as articles) should be closely coordinated, with public presentations being routinely spun off from testimony. The "media campaign" could be viewed as the third leg of our C⁴I empowerment effort, complementing Executive communications to the Hill and our coordinated T&E effort in all Marine Corps (and other service?) schools.

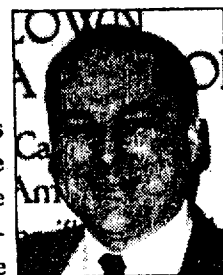
testimony--muster support for our C⁴I program while informing all concerned of our C⁴I requirements and capabilities in the broader national and joint context.

The preceding has been offered as a means of sparking discussion and suggesting some management steps which could lead to improvements in how we plan, program, and budget for Marine Corps C⁴I capabilities. It has not been offered as a prescriptive or all-encompassing view, but rather as an aid, a tool, to nurture creative and perhaps radical dialogue during the C⁴I off-site conference and subsequent implementation meetings.

MICROTIME

Robert D. Steele*President***Open Source Solutions**

Steele, a veteran of the Marines and government intelligence organizations, founded the nonprofit Open Source Solutions, saying, "Never before has the intelligence community focused so directly on the need to take greater advantage of commercial information services. It is my belief that a new relationship between government and the private sector's information brokers is going to emerge as a positive outcome of our current fiscal crisis."



In December the organization put on the first symposium on National Security and National Competitiveness: Open Source Solutions. In the course of the three-day conference, presentations ranged from Dr. James Holden-Rhodes of Los Alamos on "Divining Secrets: Open Source Intelligence in the War on Drugs" to Jane's Information Group on "An Information Vendor's Perspective on the Changing Information Environment and Opportunities for Government-Private Sector Cooperation" to John Perry Barlow on "EFF and the National Public Network."

**Industry leaders and unsung heroes
who made a difference
in the computer industry in 1992
and helped create the future**

sixth annual

Robert David Steele

KEYWORDS: Intelligence restructuring; unconventional threat and net assessments; improved threat support to acquisition; economic security, economic intelligence; author of "Ethics, Ecology, and Evolution: An Alternative Paradigm for National Intelligence"; information policy, information technology; interested in expansion of National Research & Education Network (NREN) to include intelligence community and direct unclassified interaction between intelligence analysts, business analysts, and citizen analysts, and exploitation of open sources for national competitiveness. Hispanic, fluent in Spanish.

PRESENT DUTIES: Serve as President and Chief Executive Officer of a Open Source Solutions, a non-profit educational corporation. Principal activities include sponsorship and organization of annual international symposium on "National Security & National Competitiveness: Open Source Solutions", and publication of quarterly *OSS Notices*, a means of furthering dialogue between international intelligence and information service providers. Provide short-term consultation to both government and corporate clients coping with change and adapting information services to increase effectiveness.

PUBLIC PERSONA: Named one of top 100 individuals in the information industry for 1992 by Microtimes, in recognition of year-long campaign to bring together intelligence community, traditional (corporate) information community, and non-traditional information community (brokers, hackers). Author of numerous articles on national intelligence restructuring and failures; editor of book of readings on intelligence used by Marine Corps Command & Staff College; producer of sixteen hour educational video-tape series.

PROFESSIONAL HISTORY: Eighteen years experience in national security, intelligence, and information arena. Most recently served as senior civilian in Command, Control, Communications, Computer, and Intelligence (C4I) Department, Headquarters U.S. Marine Corps (1990-1992); responsible for resource management of National Foreign Intelligence Program (NFIP) and General Defense Intelligence Program (GDIP) elements under Marine Corps cognizance, assisted with management of Tactical Intelligence and Related Activities (TIARA) program, and performed management studies across entire C4I policy, planning, and programming spectrum. Represented Marine Corps at national and defense C4I fora. Founding Special Assistant and Deputy Director of new national intelligence production facility, the Marine Corps Intelligence Center (1988-1990). Six assignments with Department of State, including overseas postings in El Salvador, Venezuela, and Panama (1979-1988). Also served two years managing artificial intelligence prototype projects, and two years in an advanced planning and evaluation group for multi-disciplinary multi-billion dollar systems. Four years experience as an infantry officer (1975-1979). Assistant instructor (AY 92-93), adjunct faculty designate (AY 93-94), Marine Corps Command & Staff College.

EDUCATIONAL HISTORY: Distinguished graduate, Naval War College (1990), Marine Corps Command & Staff College (Reserve, 1990); MPA University of Oklahoma (1987), MA Lehigh University (1976), AB Muhlenberg College (1974).

HONORS: Three personal awards, unit citation, Meritorious Honor Award for valor, Pi Alpha Alpha (national honor society for public administration).

FAMILY: Spouse Kathy Lynette; children Patrick James, Matthew Brian.

Robert David Steele

SELECTED PUBLICATIONS & PRODUCTIONS

Editor

Information Tools & Ideas (Special Inaugural Issue of extracts from the Whole Earth Review and CoEvolution Quarterly). Limited edition printing, 20 January 1993.

National Security & National Competitiveness: Open Source Solutions (Proceedings Volumes I and II, First International Symposium of 1-3 December 1992)

INTELLIGENCE Selected Readings--Book One (U.S. Marine Corps Command & Staff College, AY 92-93)

Producer

"National Security & National Competitiveness: Open Source Solutions" (Sixteen hour videotape series from First International Symposium of 1-3 December 1992)

Author

"Intelligence Primer: How to Inform Policy", awaiting placement

"General Evaluation of National Intelligence Capabilities", Intelligence and Counterintelligence Journal (forthcoming)

"The Transformation of War and the Future of the Corps", in INTELLIGENCE Selected Readings--Book One (U.S. Marine Corps Command & Staff College, AY 92-93)

"Thinking About Revolution", in INTELLIGENCE Selected Readings--Book One (U.S. Marine Corps Command & Staff College, AY 92-93)

"Information Concepts & Doctrine for the Future" (Personal Memorandum for the Deputy Assistant Secretary of Defense for Intelligence, 1 December 1992)

"E3I: Ethics, Ecology, Evolution, and Intelligence: An Alternative Paradigm for National Intelligence", Whole Earth Review (Fall 1992)

"Open Source Intelligence Clarifies Global Threats", SIGNAL (September 1992)

"Intelligence Lessons Learned from Recent Expeditionary Operations" (C4I Department, Headquarters, U.S. Marine Corps, 3 August 1992)

- "Intelligence Preparation of the Battlefield: The Marine Corps Viewpoint" (C4I Department, Headquarters, U.S. Marine Corps, 10 July 1992)
- "C4I: The New Linchpin", Proceedings (U.S. Naval Institute, July 1992)
- "Leaner Marine Corps Faces Meaner Global Challenge: Victory Will Hinge on '911' Response Teams Armed with Timely, Accurate Intelligence" SIGNAL (June 1992)
- "Corporate Information Management and Future War--Actionable Considerations" (Memorandum for the Director of Defense Information, 14 March 1992)
- "The National Security Act of 1992", American Intelligence Journal (Winter/Spring 1992)
- "National Intelligence and the American Enterprise: Exploring the Possibilities" (Draft working paper for Intelligence Policy Seminar, Harvard JFK School, 14 December 1991)
- "Applying the 'New Paradigm': How to Avoid Strategic Intelligence Failures in the Future", American Intelligence Journal (Autumn 1991)
- "Defense Intelligence Productivity in the 1990's: Executive Outline" (Official contribution to Assistant Secretary of Defense for C3I Working Group on Intelligence Restructuring, 18 May 1991)
- "Intelligence in the 1990's: Recasting National Security in a Changing World", American Intelligence Journal (Summer/Fall 1990)
- "Intelligence Support to Expeditionary Planners", Marine Corps Gazette (September 1991)
- "Artificial Intelligence and Complex Public Organizations" (MPA Paper, Virginia Polytechnic Institute, 15 December 1986)
- "Artificial Intelligence: An Annotated Bibliography" (U.S. Government Internal Publication, December 1986)
- "Strategic and Tactical Information Handling for National Security" (MPA Thesis, University of Oklahoma, April 1987)
- "Theory, Risk Assessment, and Internal War: A Framework for the Assessment of Revolutionary Potential" (MA Thesis, Lehigh University, April 1976)

NOTE: Routinely provide staff support to Marine Corps leadership preparing Congressional testimony, Marine Corps positions for Director of Central Intelligence and Director of Military Intelligence working groups, and public articles or speeches.