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 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 conventional 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 bureaucraticized 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 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:

We have paid insufficient attention to open sources...

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 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 onflict".

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

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 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 multilevel security may finally enable us to link operators directly to analysts, and break down the "green door" that has

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

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 o 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 ategy 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

Disciplines
IMINT
SIGNINT
HUMINT
OSINT

Decision Areas
Design & Methods
Funding
Collection Mgmt
Production Mgmt

Levels of Effort
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 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."

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

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 reallocating 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 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.

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

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 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.**

We urgently need a streamlined budget execution process...

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 counterintelligence 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.

****

FIRST INTERNATIONAL SYMPOSIUM: NATIONAL SECURITY & NATIONAL COMPETITIVENESS: OPEN SOURCE SOLUTIONS Proceedings, Volume I - Link Page

Previous	OSS '92 Robert David Steele, Applying the 'New Paradigm': How to Avoid Strategic Intelligence Failures in the Future (American Intelligence Journal, Autumn 1991),
Next	OSS '92 Robert David Steele, Caveat, and JFK Intelligence Policy Seminar Working Group #3, National Intelligence and the American Enterprise: Exploring the Possibilities (14 December 1991),

Return to Electronic Index Page