



[Virtual Diplomacy Homepage](#) >> [Virtual Diplomacy Publications](#) >> **VIRTUAL INTELLIGENCE**



## **VIRTUAL INTELLIGENCE: Conflict Avoidance and Resolution Through Information Peacekeeping**

by **Robert David Steele**  
President, OPEN SOURCE SOLUTIONS, Inc.

In an age characterized by distributed information, where the majority of the expertise is in the private sector, the concept of "central intelligence" is an oxymoron, and its attendant concentration on secrets is an obstacle to both national defense, and global peace. The underlying threat to peace and prosperity-the cause of causes-is the ever-widening chasm between policymakers with power, and private sector experts and participants with knowledge. Neither classified information nor information technology alone can bridge this gap-but both can make a positive contribution if they are managed within a larger information strategy which focuses on content as well as connectivity, and enables policymakers to draw upon the expertise available in the private sector. We thus require a strategy to create a "virtual intelligence community" able to both inform governance, and also carry out a new kind of virtual diplomacy, "information peacekeeping". Information peacekeeping can help avoid and resolve conflict, and represents the conceptual, technical, and practical foundation for successful virtual diplomacy-virtual intelligence "is" virtual diplomacy.

This article presents the concepts of "virtual intelligence" and of "information peacekeeping". Part I discusses the nature of conflict as an analysis problem-what do we need to know, and how. Part II reviews a number of now publicly acknowledged deficiencies of the classified national intelligence community, and makes reference to some inherent related problems in government mis-management of unclassified information. Part III examines the perils as well as the promise of information technology as now developed and applied by governments and corporations-why are we substituting technology for thinking but also, how can technology help us think and also gain access to external expertise. Finally, Part IV discusses the "information continuum" comprised largely of private sector centers of expertise; defines a theory of "information peacekeeping"; and outlines a specific strategy for creating a "virtual intelligence community" which can both inform governance, and conduct "information peacekeeping" operations-how do we harness distributed expertise from the private sector and use "tools for truth". The article concludes that the "core competency" for diplomats, whether real or virtual, must be the management of information *qua* content-its discovery, discrimination, distillation, and dissemination as intelligence. It follows from this that diplomats must take the lead in developing a national information strategy as an element of national power, and also master the art of "information peacekeeping".

### Part I: What Do We Need to Know, and How?

The policymaker needs an intelligence-support system which is directly related to their daily schedule; which provides just enough intelligence just in time, at the lowest possible level of classification; and which enables direct access to private sector experts whenever needed. This system must be firmly grounded on a foundation of complete global geo-spatial data at the 1:50,000 level, and must provide the policymaker with both strategic generalizations and a full range of multi-dimensional assessments, which include a full understanding of the cultural, technological, and geographic aspects of a potential or on-going conflict. Organizationally, this system must fully integrate the information available to civilian, military, and law enforcement authorities as well as

business leaders; and it must offer a seamless architecture which transitions easily from domestic to international locations under conditions of both peace and war. Above all, it must allow the policymaker to deal with emerging threats on a "come as you are" basis, and to harness private sector expertise in real-time.

**Unclassified Intelligence.** Intelligence is information, which has been discovered, discriminated, distilled, and disseminated in a form tailored to the needs of a specific policymaker at a specific time and place. Intelligence is most often *not* classified, and its utility in fact decreases dramatically with every increase in its level of classification. In today's global environment, intelligence which can be shared and which does not compromise the political standing of the sponsors of the intelligence by relying on covert means, is critical.

TECHNOLOGY IDEA: Require every "intelligence" report to offer varying degrees of classification beginning with unclassified, to clearly mark all paragraphs with their inherent level of classification, to footnote primary and secondary customers and their telephone numbers, and to specify in detail the open sources and experts as well as the classified sources which were drawn upon to create the report. Provide consumers with an electronic means of documenting whether they actually read the report, and an electronic means of grading the report (at its various levels) in real time.

**Just Enough.** The policymaker does not have the time or the inclination to digest vast quantities of information, however much they may feel that only their intellect could possibly comprehend all the nuances. The successful analyst supporting the policymaker will have gained their trust and understanding, and will provide "just enough" intelligence to permit the policymaker to grasp the essence of the value-added information (i.e. insights the policymaker did not already have), and to provide the analyst with guidance if additional detail or other related analytical paths are to be pursued.

TECHNOLOGY IDEA: Require that intelligence be delivered via Web-like applications which begin with a paragraph and allow the policymaker to drill down to a page or a longer document, or to navigate into original sources if desired. This is completely distinct from the "Intel-Link" concept, which does nothing more than convert the intelligence production fire-hose into electronic form. This idea also requires aggressive commitment to the digitization of supporting documentation, and hence facilitates inter-agency access to basic multi-media and multi-lingual raw information sources. This idea can be applied on behalf of the large number of policymakers who require hard-copy products, by automating the production process so that four levels of details are provided.

**Just in Time.** Twelve month research plans and eighteen month editing cycles have made most "intelligence" (actually no more than classified information) irrelevant to the day-to-day needs of the policymaker. The policymaker needs intelligence that is pertinent to the decisions they are making that very day (including decisions, which set in motion longer term endeavors by others).

TECHNOLOGY IDEA: To the extent that the policymaker is willing (some operators are worse than spies in their obsession with secrecy), ensure that the daily agenda of the policymaker is electronically available to all analysts supporting them, kept up to date, and used as the electronic "hot link" foundation for providing intelligence support. As the policymaker looks at their daily agenda on their screen, they should see a little "icon" that says, in essence "Intelligence Available", and from that be able to go directly to a paragraph, then a page, and then to supporting documentation.

**Direct Access.** In the 21<sup>st</sup> century, the "acme of skill" for the master analyst will be the ability to put a policymaker with a hot question in direct touch with a world-class expert (generally in the private sector) who can create new knowledge on the spot, and in a few minutes "cut to the chase" and provide the policymaker with an informed judgement in real time that is tailored to the precise nuances of concern to the policymaker.

TECHNOLOGY IDEA: Using existing Web technology, including security technology, establish a "virtual intelligence community" directory which is constantly updated by the Institute of Scientific Information, and permits any analyst or indeed any policymaker to quickly identify world-class experts in any topical area.

**Earth Map.** The policymaker, counterparts, and staffs all require an accurate map of those portions of the earth under consideration at any given time. This is not only essential as the foundation for decision-making, it is critical as the foundation for fusing information from various collection disciplines (imagery, signals, human) and for automating the visualization of information in the aggregate. Hard as this is for most Commanders-in-Chief and their staffs to understand, none of us have the world mapped accurately or comprehensively. The United States has less than 10% of the world mapped at the 1:50,000 level (10 meter resolution with contour lines), and most of that is severely out of date. In both Somalia and Burundi, the next best alternative to tourist maps has been previously classified Soviet military topographic maps at the 1:100,000 level, only recently made available through a U.S. company, East View Publications.

TECHNOLOGY IDEA: Earmark \$250 million dollars a year to the Department of State with which to procure commercial imagery sources and related processing services in support of both peacekeeping initiatives and EARTHMAP Report requirements of other civilian agencies. These commercial imagery sources will still require orientation (ortho-rectification) using either precision imagery from the National Reconnaissance Office or positioning of key features using hand-held Global Positioning System (GPS) receivers, but such a fund would be responsive to civilian and peacekeeping requirements without being subject to realignment by unappreciative intelligence and defense bureaucrats, and would help resolve decades of active neglect in this area.

**Strategic Generalizations.** The policymaker requires strategic generalizations with which to plan and direct operations. Analysts and their managers too frequently inundate the policymaker with thousands of "current intelligence" updates, and also exaggerate the threat, for lack of a model of analysis which requires them to address the peacekeeping environment in a comprehensive manner which readily brings out useful generalizations.

- 
- In 1989, after the Marine Corps Intelligence Center was established, a review of existing Central Intelligence Agency (CIA) and Defense Intelligence Agency (DIA) was found to contain no intelligence of general value to the Marine Corps. Everything was a "snapshot" (generally dated) of a specific weapons system, personality, organization, event, or location.
- A more useful model for integrated analysis was developed, and tested, with the finding that *the threat changes depending on the level of analysis, and also upon the relationship between the military capability being considered, and the pertaining civil and geographic factors in the area of operations.*

- Below is a high-level view of the model:

	Military	Civil	Geographic
Strategic	Sustainability: Ability to sustain operations over time and space	Allies: External relationships of strategic import	Location: Strategic geo-political location or source of materials
Operational	Availability:	Instability:	Resources:

	Quantities of military power available for commitment	Internal precipitants and preconditions of volatility	Internal natural resources affording self-sustainment
Tactical	Reliability: Impact of training and maintenance on existing capabilities	Psychology: Internal group dynamics affecting cohesion and operations	Terrain: Internal geographic conditions affecting mobility
Technical	Lethality: Effectiveness of specific capabilities assuming no constraints	Infrastructure: Transportation, power, communications, and other infrastructures	Atmosphere: Internal climate affecting system performance

Figure 1: Concept for Integrated Intelligence Analysis

Two examples of this model's utility are offered because its implications are so important to policymakers dealing with complex conflict situations.

**Middle Eastern Tank Threat.** In a test case discussed with the appropriate analysts from all of the major intelligence agencies in the U.S. governments, we discovered that the tank threat in a particular Middle Eastern country, historically classified as *high* because it was comprised of Soviet T-72 tanks, at the time the most powerful main battle tanks outside our own, changed dramatically depending on the level of analysis—it was only *high at the technical level (lethality)*.

- **At the tactical level (reliability)**, because of very poor troop training, the long-term storage of most tanks in warehouses, and the cannibalization of tanks at random for parts, the threat fell to *low*;
- **At the operational level (availability)**, because of the quantity of tanks scattered around the country, the threat rose to *medium*; and
- **At the strategic level (sustainability)**, where various constraints would not permit this country to sustain tank operations for more than two weeks, the threat again fell to *low*.

We considered this very significant to the perspective of the policymaker or commander making decisions about the over-all structure of the force to be deployed to this region, even in the absence of related information about civil and geographic factors.

**Integrated Analysis.** In a second example, which illustrates the importance of civil and geographic factors to the over-all analysis of any peacekeeping situation or related acquisition and employment decisions, the Commandant of the Marine Corps asked us to evaluate the Marine Corps requirement for a follow-on procurement of the M1A1 tank. We examined civil and geographic factors for the sixty-nine countries (now eighty) which comprised the expeditionary environment, and discovered these "strategic generalizations":

- **Intervisibility (Line of Sight Ranges).** 91% of the countries in the Marine Corps environment offered line of sight distances of 1,000 meters or less, making the M1A1 irrelevant to operations in those countries;
- **Cross-country mobility.** 79% of the countries offered *zero* cross-country mobility; the terrain would require all mobility platforms to use normal roads (most of which have bridge loading limitations of 30 tons or so, making the M1A1's 70 ton weight a distinct liability);
- **Ports.** 50%-fully half-of the countries did not have a port usable by a U.S. Navy or Maritime Pre-Positioned Force (MPF) ship-they lacked an adequate depth, turning radius, and/or piers and cranes. This means that the 70-ton M1A1 would have to be off-loaded in mid-stream using scarce and often-inadequate landing craft.

A similarly strategic observation was subsequently made with respect to aircraft, which are designed by the U.S. Navy for the U.S. Marine Corps based on a standard aviation day that is warm (around 65°F) and with average humidity.

The Marine Corps aviation day is in fact *hot* (routinely over 80°F) with very high humidity. Translation: Marine Corps aviation can carry half as much half as far than the book says it can-both range and lift are dramatically reduced under these conditions. Yet policy makers and the military commanders that advise them consistently fail to plan for these civil and geographic realities. This is of special concern with respect to Non-Combatant Evacuation Operations (NEO).

We also discovered that :

- most U.S. Embassies were well beyond the round-trip range of the CH-46 from a naval platform at the five fathom line even at optimal performance;
- most countries in the Third World can out-gun the standard U.S. Navy five-inch gun with their existing shore batteries; and
- we are completely lacking in digital imagery and 1:50,000 combat charts for operations in 90% of the world, as well as 200 ship-years behind in shallow-water (100 fathom and less) hydrography.

Why is this so important? The sad fact is that policymakers are often ignorant of the realities of the military, civil, and geographic elements in relation to one another and the levels of analysis, and this ignorance leads to woefully inadequate estimates of what it will take to achieve stated objectives. At the same time, the military is uninformed as to the "intangible" aspects of the situation, and generally is not trained, equipped,

and organized for operations which require that they deal with people rather than kill them.

TECHNOLOGY IDEA: Post the Marine Corps study as a public document.

**Multi-Dimensional.** Consider the following table:

	Political-Legal	Socio-Economic	Ideo-Cultural	Techno-Demographic	Natural-Geographic
Perception	Isolation of elites; inadequate intelligence	Concentration of wealth; lack of public disclosure	Conflicting myths; inadequate socialization	Acceptance of media distortions; inadequate mass education	Reliance on single sector or product; concentrated land holdings
Identity	Lack of elite consensus; failure to define priorities	Loss of economic initiative; failure to recognize need for balanced growth	Loss of authority; failure to provide and honor national myth system	Failure to accept and exploit new technologies and new groups	Failure to integrate out-lying territories into national system
Competence	Weak or inefficient government; too much or too little bureaucratization	Break-down of fiscal, monetary, development, or welfare policies	Humiliation of leaders; loss of confidence by population	Failure to enforce priorities, with resulting loss of momentum	Failure to prepare for or cope with major natural disasters
Investment	Ego-centric or parochial government	Excessive or insufficient mobility; lack of public sector	Cynicism; opportunism; corruption	Failure to nurture entrepreneurship or extend franchise to all groups	Failure to preserve or properly exploit natural resources
Risk	Elite intransigence; repression; failure to recognize new sources of power	Failure to deal with crime, especially white collar crime	Failure to deal with prejudice; desertion of the intellectuals	Failure to develop national research & development program	Failure to honor human rights; failure to protect animal species
Extroversion	Ineffective tension management; failure to	Structural differentiation; lack of national transportation	Elite adoption of foreign mores; failure to deal with	Failure to develop communications infrastructure, shared images	Failure to explore advantages of regional integration

	examine false premises		alienation		
Transcendence	Foreign control of gov't; arbitrary and excessive government	Loss of key sectors to foreign providers; loss of quality control	Media censorship; suppression of intellectual discourse	Failure to control police, army, or terrorists; failure to employ <i>alphas</i>	Failure to respect natural constraints or support organic growth
Synergy	Failure to assimilate all individuals or respond to groups	Status discrepancies; lack of economic motivators	Absence of sublimating myths; failure of religion	Failure to provide program and technology assessment	Failure to distribute political benefits between urban and rural
Complexity	Garrison, industrial, or welfare states	Unstable growth; external diseconomies; excessive DoD \$\$	Cultural pre-disposition toward violence; fanatic elements	Excessive urbanization, pollution, nuclear development	Lack of land for expansion, inefficient land use or land tenure

Figure 2: Framework for the Observation of Conflict

The policymaker is poorly served when analysts focus only on the political-legal situation, or the military situation, or even-to the extent they can gain access to the necessary open sources-on the economic situation. Every emerging and on-going conflict has a multi-dimensional nature, and must be understood across a spectrum, which includes ideological, cultural, technological, demographic, natural, and geographic conditions. At the same time, culturally astute experts must study the aspects of human development and the local psychology, and these informed judgements factored into the decision-making process.

The average analyst, pre-occupied with cutting and pasting miscellaneous "current facts", and lacking access to sources of cultural and other forms of "intangible" intelligence as well as access to tools for visualizing complex integrated problem sets, is rarely if ever going to provide the policymaker with insights into the multi-dimensional nature of the conflict and the consequently unanticipated consequences of revolutionary change in the non-traditional dimensions such as the ideo-cultural or techno-demographic.

TECHNOLOGY IDEA: First, do a case study of a single country, and completely re-define the idea of a "Country Study" so as to move far beyond the cursory coverage of the CIA World Fact Book or the useful but largely "tangible" Army Country Studies. Then develop a Web-based network of sites and publications organized by country and within country so as to allow any policymaker to quickly access multi-lingual and multi-cultural perspectives in each of these matrix areas, using only open sources of information which can be easily shared with coalition and non-governmental partners. Use automated gisting and clustering technology to quickly visualize the aggregate data while comparing "points of view" from different sites and organizations.

**Emerging Threats.** There are two aspects to the changing nature of the threat as we approach the 21<sup>st</sup> century, and both merit brief discussion because the lack of knowledge among policymakers, and the mind-set inertia of the analysts supporting them, suggest that we are avoiding making significant changes to how we direct, collect, process, and analyze information, and this will continue to generate "intelligence failures".

First, it is important to recognize the dramatic difference between the conventional threat that everyone has grown comfortable following since the end of World War II, and the emerging threats which we are not trained, equipped, or organized to identify and evaluate.

The *conventional threat* has been governmental in nature, comprised of conventional and sometimes nuclear forces arrayed in a static order of battle, developing their capabilities linearly over time, fighting by known rules of engagement, with known doctrine, providing ample strategic warning of attack, and using known intelligence assets.

The *emerging threat* is generally non-governmental, unconventional, dynamic or random in event initiation, non-linear in its development due to the availability of off-the-shelf equipment, fighting without any constraints or rules of engagement, with unknown doctrine, with no established indicators of attack, and with an unlimited fifth column.

Second, it is important to reflect on how the emerging threats, looked at in a different manner, require a completely different form of "intelligence" as well as a completely different form of "defense" organization.

**High-Tech Brutes** are the ones we understand, and are represented by the conventional powers. They practice medium and high intensity warfare, have as their source of power money, and rely on physical stealth and precision targeting of munitions for their effect.

**Low-Tech Brutes** are the ones we are beginning to fear, and are represented by the transnational terrorist and criminal organizations. They practice low-intensity conflict, have as their source of power ruthlessness, and rely on natural stealth and random targeting for their effect.

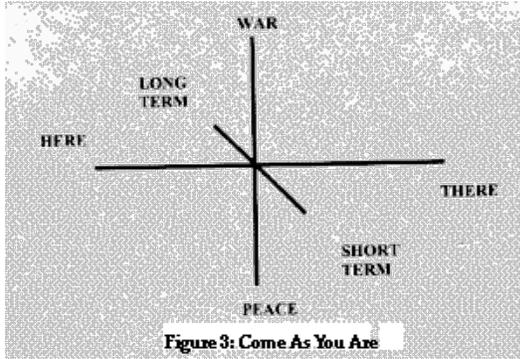
**Low-Tech Brains** are the "wild card" of history, and are presented by the Islamic Fundamentalists (who merit respect for their religious beliefs) and also cults (which do not merit religious status). They practice Jihad, have as their source of power ideology, and rely on mental stealth and mass targeting for their effect.

**High-Tech Brains** are the threat *de jure*, and are represented by friendly and unfriendly nations practicing economic espionage, transnational corporations exercising electronic privateering, and individual information terrorists and information vandals as well as criminal hackers stealing what they can from an unwitting world of nations, corporations, and citizens. They practice information warfare, have as their source of power knowledge, and rely on cyber-stealth and database targeting for their effect.

TECHNOLOGY IDEA: Establish an inter-agency working group, with extensive representation from the private sector and especially including law enforcement, hackers, and non-governmental organization analysts, and devise a completely fresh directory of "indications and warnings" for the three threat categories that comprise the unconventional threat. Undertake an effort to automate multi-lingual content analysis, including the digitization of important foreign language publications not now covered by the Foreign Broadcast Information Service (FBIS) and unlikely to be widely monitored.

**Come As You Are.** Finally we must come to grips with the fact that "the water's edge" is as dangerous to our security as the "iron curtain" once was, in that it is imposing-on our governmental policy organizations, and on our national and law enforcement intelligence communities-a dangerous and likely catastrophic barrier to the development of seamless lines of communication and shared knowledge about transnational criminal gangs and terrorist organizations moving freely between overseas and domestic locations; major religious as well as cult organizations and alien-smuggling operations; and individuals participating in economic espionage, information terrorism, and information vandalism, in association with international partners, be they governments, corporations, gangs, or other individuals. Consider the following

illustration:



What does this chart mean to how we devise policy and execute operations? It has two meanings:

First, it demonstrates the urgency of creating a seamless architecture for linking policymakers, financial authorities, law enforcement, the military, and all others including non-governmental organizations, into a global information network where shared knowledge is the foundation for preventing conflict and damage to mutual interests including financial stability. Conflict is no longer simply unilateral, military, or "over there".

Second, it emphasizes that conflict avoidance and resolution against the emerging threats represent "come as you are" situations, and that we do not have the luxury of time to gradually recognize threats, devise means of monitoring them, and finally come to consensus on means of dealing with them, after which the means can be gradually constituted. An underlying implication of this lack of time is that we must find a means of harnessing all available citizens as voluntary sensors in a global "warning system", and that we must engage all available expertise from the private sector so as to be able to respond rapidly to threats beyond the ken of the conventional government policymaker, bureaucrat, or analyst.

What does this mean in terms of what we need to know, and how? It means that we now have to cover a much vaster range of "threats" (and also opportunities), each much more subtle, more diffuse, more obtuse, than the traditional conventional threat we have grown to rely on for our feeling of security (that we understand our world). As we shall see in the next section, the U.S. Intelligence Community is neither prepared, nor inclined to become prepared, for this more complex world. At the same time, the private sector now offers a "virtually" unlimited range of open sources, systems, and services, which are directly applicable to meeting the needs of international policymakers, and which have the added advantage of avoiding the constraints associated with classified information.

## Part II: Why Don't We Know What We Need to Know?

*The policymaker today suffers from a triple liability: an intelligence community optimized for processing secrets out of context (without adequate access to open and especially multi-lingual sources of information); a government information handling system unable to deal with the flood of unfiltered and unanalyzed information directed at the policymaker from hundreds of international advocacy sources all pressing their own agenda; and a policy process which is inherently focused on domestic political decision criteria acted upon with little time for reflection.*

No person who really understands the roots of the intelligence function in support of policy can fail to be dismayed by the existing situation. Both the Office of Strategic Services (OSS) and the Central Intelligence Agency (CIA), relative newcomers to the global intelligence community, were created to carry out strategic intelligence analysis and to coordinate inter-agency information and intelligence assessments. Both were intended on inception and into the future to rely predominantly on open sources. Unfortunately, the allure of clandestine operations and then the failure of these same clandestine operations against the Soviet Union, led the United States to invest very heavily in narrowly focused satellite technology, to the detriment of both its clandestine human intelligence collection capability, and its severely degraded analysis capability.

In general terms, the U.S. Intelligence Community fails to meet the needs of the policymakers because:

1. It is optimized for secrecy and does not have adequate access to the substantive, contextual, and culturally critical information available from open sources-it cannot claim, with credibility, to be "all source" because of its gaps in access to multi-lingual open sources.
2. It is extremely dependent on overhead satellite collection assets and severely lacking in commensurate investments in data processing, human clandestine collection, and human analysis capabilities.
3. It is completely isolated from the larger worlds of government and private sector information and intelligence-by inclination in terms of management and culture, and by design in terms of budgets and technology.
4. It persists in using a priorities-driven requirements system in which repetitive collection against generically monitored high-priority targets (e.g. Russia, China, Iraq) consistently eliminates the possibility of even the most cursory coverage of specific aspects of Third World and other lower-priority targets.
5. It lacks a model of analysis and a process of analysis.

Consider this table:

Quick Looks	Direction	Collection	Analysis	Dissemination
Strategic Customers: 1. Policymakers 2. Coalition Partners 3. Acquisition Managers 4. Public 5. Media	No tracking system for consumer satisfaction; no integrated multi-disciplinary requirements database; non-traditional consumers not well represented.	Superb but ossified technical capability with limited utility against emerging threats. Very deficient human (clandestine) and open source capabilities.	Cut-and-paste community, a few bright lights kept under tight control, too many young people with little idea of overseas realities and with very limited language/cultural skills.	Cumbersome compendiums of limited utility to day-to-day decisions.
Operational Customers: 1. Theater commanders and staffs 2. Embassy Country Teams 3. Coalition Partners	Self-imposed overemphasis on "worst-case" threats continues, with almost complete lack of focus on such basics as Third World mapping data and communications intelligence.	Virtually no support for human contingency requirements, limited low intensity conflict indications and warning capability.	Highly motivated and responsive analysts in the joint intelligence centers, but without adequate access to open source information and especially information in host country	Excellent dissemination to the theater headquarters, very poor capability to support theater (forward), Joint Task Force commanders, or Country Team members.

4. Media			foreign languages.	
Tactical Customers: 1. Tactical Military Commanders 2. Non-governmental organizations 3. Host governments 4. Media	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.	Adequate organic capabilities with the exception of wide-area imagery; ground reconnaissance skills appear to have atrophied; completely inadequate prisoner and refugee handling.	Mixed bag, with personnel generally consumed by volumes of traffic and additional duties-overloaded with raw data, and very inadequate hardware and software.	Lack of realistic communications architecture for sharing data with coalition and civil counterparts, lack of digital mapping data, very vulnerable to electronic attacks at source (home front) and in field.
Technical 1. Tactical commanders and pilots 2. Acquisition project managers 3. Vendors	Well-established mechanisms but not always focused on the right questions. Slow to focus on C3I vulnerabilities.	Very good against denied areas, less so against rogue states, emerging non-state actors, and present-day allies and their religious partners.	Too much emphasis on technical countermeasures and single system threat assessments, with no strategic generalizations.	Adequate in relation to fixed sites; will be completely inadequate when "tactical" technical collection and analysis is needed.

Figure 4: Critical U.S. National Intelligence Deficiencies

In systemic terms, in relation to the four major functions of intelligence and in relation to the four major consumer groups, the U.S. Intelligence Community is not trained, equipped, and organized to be effective against the complex threats *and opportunities* which face U.S. policymakers and their international partners today.

What about with respect to the vaunted individual disciplines or aspects of classified intelligence which are intended to provide policymakers with "plans and intentions" intelligence as well as a full gamut of encyclopedic intelligence, current intelligence, indications & warning intelligence, estimative intelligence, general military intelligence, and scientific & technical intelligence? Below are some unclassified extracts from the evaluative comments that received policy and security approval within the Marine Corps but were never published:

- 
- **General Military Intelligence (GMI) Production.** More attention should be devoted to integrating intelligence about operational geography and civil factors pertinent to military operations into over-all estimates.
- **Scientific & Technical Intelligence (S&TI) Production.** Our Service planners and programmers would benefit from expanded analysis of S&TI function to include Third World arms production programs, weapons sales and thefts, and technology transfer. We look for improved integration of both HUMINT reporting and annotated imagery into S&TI production. S&TI databases on the Third World appear lacking.
- **Indications & Warning (I&W).** Many non-military crises require a commitment of military resources for stability or humanitarian reasons. We are concerned by the absence of an estimative methodology and dedicated resources for anticipating such crises. Our community must have a "peacetime engagement" indications & warning capability, together with a capability to produce estimates relevant to national security planning and programming for Third World stability operations.
- **Human Intelligence (HUMINT).** There are several general trends of concern: the most fundamental is that the existing national intelligence capability is simply not able to meet our needs for military and non-military plans and intentions; nor can it provide for contingency support, and stay-behind ground reconnaissance and support assets. This is especially the case in the Third World.
- **Signals Intelligence (SIGINT).** The proliferation of commercial technology, the reduction of our overseas basing infrastructure, and the rapid emergence of multiple threat groups in new areas of concern (e.g. criminal and narco-revolutionary splinter groups in areas of the world not previously covered) will make it extremely difficult for the SIGINT community to realign its resources and develop new capabilities with the declining dollars it receives under the defense draw-down. The SIGINT community is beset by other challenges, including a lack of qualified linguists for many lower priority languages.
- **Imagery Intelligence (IMINT).** The emergence of multi-spectral imagery (MSI), and its commercial availability, together with possible economies achievable by modifying airborne targeting radar, offer innovative alternatives for meeting some of our most pressing requirements.
- **Collection Management.** Our national intelligence community must strive to establish a national requirements system that is useful in the management of resources, is cross-disciplinary, automated, and is responsive to individual customers by allowing them to track their requirements resolution by discipline, country, topic, and time frame.
- **ADP and Intelligence Communications.** The intelligence community as a whole must have a global data-driven C4I2 architecture, which encompasses all mission areas and provides for multi-level communications and computer security oriented toward near-real-time sensor-to-shooter support in

Third World operations. The same architecture must also satisfy our requirements for intelligence and information sharing with U.S. law enforcement, foreign military, and non-governmental humanitarian organizations.

- **Processing and Dissemination.** Processing and dissemination management (and concepts) cannot be isolated from ADP and Intelligence Communications management. This is also true of production planning-advances in technology and the manner in which multi-media data can be handled have finally made "product" and "system" two sides of the same coin; our planning processes in these area must be integrated.
  
- **Intelligence Training.** We would welcome more emphasis on the development of advanced analysis methods and tools throughout the community, and development of a means of exporting these methods and tools to all intelligence analysts. We also need to do a better job of educating non-intelligence professionals regarding all aspects of intelligence, including how to ask for intelligence, how to collect it, and what are the capabilities and limitations of our existing and planned intelligence systems.

Now, lest one conclude that the U.S. Intelligence Community is to blame for its inability to adequately inform the policymaker, it is time to stress several factors which permit its deficiencies to persist:

1. The budget for intelligence operations is not subject to critical review in detail, obscuring virtually everything in its "base" budget and being limited to scrutiny by a few staff employees of the Senate Select Committee on Intelligence (SSCI) or the House Permanent Select Committee on Intelligence (HPSCI).
2. The majority of the budget for intelligence operations is managed by the Secretary of Defense rather than the Director of Central Intelligence, and is such a small amount in relation to the total Department of Defense budget as to merit very little oversight from the Secretary of Defense.
3. The budget is not subject to review by the various policy-level consumers in the Administration, to whom "intelligence" represents a "free good" which they may ignore, or consume, at their pleasure. A corollary of this point is that the policymaker is permitted to avoid investing in their own analysts (e.g. the Departments of Treasury and Commerce have mediocre to non-existent intelligence collection and analysis organizations).
4. No one in Washington is held accountable for ignoring intelligence, and in fact most intelligence is presented in a fashion which makes it not only easy to ignore, but essential: as a cumbersome compendium of classified research, often so compartmented that the executive assistants are not cleared to read it, but so difficult to gain access to (codeword signatures, special vaults) that the policymakers don't bother to seek it out.
5. The needs of the policymaker, and the wont of the intelligence analysts, are worlds apart. Four contrasts between the two worlds are provided:

- The analyst focuses on all-source INTERNATIONAL DATA while the policymaker focuses on DOMESTIC POLITICAL ISSUES as the primary criteria for decision-making.

The analyst focuses on (and is driven by community managers to) produce "PERFECT" products over a lengthier timeframe while the policymaker 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 policymaker 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 focus on SUBSTANCE and ACCURACY while the policymaker focuses on POLITICS and PROCESS, an arena where disagreement can be viewed as insubordination. Even if new information is received, political considerations may weigh against policy revision.

1. Lastly, the sources of unclassified (and unanalyzed) information available to the policymaker drown out and reduce to almost nothing the impact of the narrow inputs from classified intelligence. Consider these competing influences on the policymaker, all flooding the policymaker with verbal and written information:

- 
- Politicians (Executive Leadership, Legislative Leadership, Personal and Professional Staffs)
  
- Government Officials (Department Heads, Assistant Secretaries, Program Managers, Message Traffic)
  
- Foreign Officials and Organizations (Diplomats, Counterparts, Correspondence)
  
- Private and Public Sector (Lobbyists, Executives, Citizen Groups, Pollsters, Individuals)
  
- Independent Researchers (Think Tanks, Academics, Authors, Foundations, Laboratories)
  
- Media (CNN/C-SPAN, Newspapers, Wire Services, Radio/TV, Pool Reporters)
  
- Personal (Family, Intimates, Church, Clubs, Alumni)
  
- Intelligence Community (CIA, DIA, NSA, NRO, NIMA, FBI, State INR, Service Intelligence organizations)

What does this all mean? It means that right now the U.S. Intelligence Community is unable to meet the most practical needs of the policymaker, at the same time that the policymaker is unable to define and manage their own needs in the context of their available funding for unclassified information procurement, and their prerogatives as intelligence consumers to dictate a new focus for national intelligence—one which stresses responsiveness to policymakers and the exploitation of open sources of information. Neither the U.S. Intelligence Community, nor the information management specialists serving the policymakers, nor the policymakers themselves, have focused on the basic fact that intelligence is an inherent responsibility of command, and it is the *policymaker* who must specify the timing, format, length, and level of classification of the intelligence products they wish to receive—to abdicate this responsibility is to persist in a condition of power without knowledge.

### Part III: The Perils and Promise of Information Technology

Information technology up to this point has been a resource drain, and ultimately reduced the ability of

government to hire and retain world-class experts. Information technology has imposed on the policymaker financial, productivity, secrecy, and opportunity costs. The "iron curtains" between classified information technology systems, policymaker information technology systems, and private sector information technology systems have created a wasteful and counter-productive archipelago of information, which the policymaker needs but cannot access electronically. Billions of dollars are being wasted through a lack of coordination and standardization, and a lack of focus on requirements analysis, human productivity, and the need for easy access to multiple remote multi-lingual and multi-media databases. Information technology continues to offer extraordinary promise, but only if the policymaker begins to manage the technology rather than abdicate technology procurement decisions to technologists far removed from the core competencies of the policy environment.

Information technology, in relation to "content", appears to have swamped the end-user with three waves, each of which has left the end-user less productive and less informed than they were before having information technology imposed on them.

The "first wave", when electronic publishing and electronic storage of data first became possible, brought with it two major negatives:

Because computer memory was so limited, the end-user was turned into a "virtual slave" to the computer, and obliged to master all manner of arcane commands with which to feed the "c prompt"; and

Because librarians were focused on hard copy, and technologists were focused on processing generic bytes, the computer industry developed without any strategy for data classification and data archiving.

The "second wave", when increasingly sophisticated word processing and database management programs became available, also brought with it two major negatives:

Because the programs were so sophisticated, end-users were required to either spend a significant amount of time in training, or to forego most of the features offered by the programs; and

Because the programs kept changing and managers kept allowing the technologists to specify ever-more sophisticated programs for use, the end-user ended up losing access to much of their legacy data, and spending a great deal of time re-entering data to satisfy the changing formats and features of the new programs.

Now comes the "third wave", in which the Internet is touted by the most optimistic as well as the least principled (two different classes of advocate) as the be-all and end-all for meeting the information needs of the policymaker, with, again, two major negatives:

Because the Internet is such an interesting environment, and new programs do indeed have a lot of power, analysts are disappearing into the void, either hopelessly lost or hopelessly addicted to wandering in cyberspace; and

Because the Internet does offer a superficial amount of information on virtually any topic, albeit with no real source authentication or validation, it has become the "classic comics" of knowledge, and too many policymakers and their analysts are accepting the Internet as the first *and* last stop in their quest for information.

As one reflects on the \$300 billion dollars (roughly) that the U.S. Intelligence Community has spent primarily on information technology, and the \$3 trillion (roughly) that the rest of the U.S. Government has spent on information technology (including weapons and mobility systems information technology), four "costs" emerge which must be considered by policymakers as they plan future investments in information technology:

**Financial costs.** The ugly fact of the 1980's and 1990's is that information technology usually provides a *negative* return on investment in both government and corporate applications, largely because of the dramatic negative impact on employee productivity, and because of the lack of standardization across organizational

lines which interferes with data sharing and also wastes resources through the development of multiple variations of complex systems responding to different managers with the same functional requirements.

**Productivity costs.** The productivity costs of badly managed information technology acquisitions are two: the loss of employee productivity due to constantly changing applications; and the loss of organizational productivity due to an absence of attention to external sources of information.

**Secrecy costs.** Between classifying our vulnerabilities and classifying our data, we have left ourselves vulnerable to electronic attack of our financial, communications, power, and transportation infrastructures in the private sector, at the same time that we have deprived most end-users of critical information. There is also "virtual secrecy", a pervasive compartmentation and concealment of information from the public and indeed from the policymakers, which results from poor information management practices as well as bureaucratic regulations that block access to unclassified information.

**Opportunity costs.** Between spending billions of technical collection and related security systems, and policies which ensured the technical isolation of analysts dealing predominantly with classified information and analysts dealing predominantly with unclassified information, we have essentially created a dysfunctional technological architecture—we have created a "virtual" iron curtain between sectors (government, business, media, academy); a "virtual" bamboo curtain between institutions within sectors (Oxford, Harvard, Stanford, George Mason, University of Southern Florida); and a "virtual" plastic curtain between individuals who cannot readily share word processing or graphics files. This dysfunctional technological architecture is preventing policymakers from identifying opportunities for conflict avoidance in time to be effective, and at a far lower cost in terms of political and economic resources than will be required later to resolve the conflict once begun.

In summary, today information technology is part of the problem, not part of the solution. However, the fault does not lie with the technologists, but rather with the managers who have abdicated their responsibility for the direction of technology and its proper applications in support of core competencies.

**At the strategic level,** we must manage information as the core value—what Paul Strassmann calls "knowledge capital<sup>TM</sup>", and use information technology to reach across national, organizational, and disciplinary boundaries.

**At the operational level,** we must radically alter how we manage both security and procurement, as both are now hobbling information technology by placing barriers in the way of connectivity and state of the art capabilities, while we simultaneously avoid investing in advanced electronic security programming.

**At the tactical level,** we must dramatically realign dollars from the collection of classified information, to the discovery, discrimination, distillation, and dissemination of unclassified information.

**At the technical level,** we must accept that our classified base of analyst workstations is a given and stop trying to create a duplicate architecture of unclassified machines which the analysts and policymakers will never use—instead we must rely on private sector Sensitive Compartmented Information Facilities (SCIF) to serve as the "air gaps" for introducing unclassified information into the classified system. At the same time, we must invest in our global Embassies (of all nations) and their related corporate offices, and establish a Global Information Management (GIM) concept of operations.

Returning to the field of imagery and global geospatial data to illustrate the perils of badly managed information technology, one can observe:

Billions have been spent to collect repetitive snap-shots of (then) Soviet missile silo doors, at the same time that the mapping satellite constellation was cancelled and the Defense Mapping Agency was forced to create an enormously cumbersome processing system to digest synoptic and relatively microscopic classified images. The system is also poorly suited to integrating commercial imagery sources that have now far outpaced national assets in terms of diversity of utility and breadth of availability.

SPOT Image Corporation has most of the earth already in its archives, generally 100% cloud-free, and less than three years old. Yet the U.S. Intelligence Community refuses to realign funds to meet the stated need of the National Imagery and Mapping Agency (NIMA) for \$250 million dollars a year to buy commercial imagery; the Office of the Assistant Secretary of Defense has refused an even more modest request from NIMA for \$25 million a year; the Director of Central Intelligence continues to refuse to create a separate funding line for the procurement of commercial imagery; and NIMA compounds this problem by refusing to acknowledge the EARTHMAP Report and the needs of the Departments of State, Commerce, Treasury, and other key elements of the government concerned with peace and prosperity.

In the absence of a means for integrating *existing* commercial global geospatial data into a global multi-media database, automated data fusion between distinct sources and disciplines remains an impossibility. *Global geospatial data at the 1:50,000 resolution level is literally the foundation for information sharing and integration and automated value-added processing and-ergo-the foundation for virtual intelligence, virtual diplomacy, and information peacekeeping.*

Now what of the promise of information technology? One can focus on two areas: generic functional requirements for individual workstations; and generic organizational methods for routine, reliable, and responsive access to global data and expertise-neither exist today.

The single most helpful contribution to the productivity of all those supporting policymakers across national and organizational boundaries would be the stabilization of their individual workstations and their means of accessing multi-lingual and multi-media data. At a minimum, organizations must put a stop to the practice of duplicative and counter-productive investments in varying kinds of "all source fusion workstations" which ultimately divide rather than unite data and people.

<p>Data entry</p> <p>Selective text and image extraction</p> <p>Hard copy scanning including color</p> <p>Audio transcription/translation</p>	<p>Data routing and records management</p> <p>Automated clustering of related information</p> <p>Automated gisting</p> <p>Automated weighting of documents for review</p> <p>Automated routing, filing, and purging</p>
<p>Data retrieval</p> <p>Very large unstructured multi-media database search</p> <p>Automated access to and querying of distributed databases</p> <p>Menu-driven multiple database/multi-level security access programs</p> <p>Natural language query conversion to all legacy search systems</p> <p>Automated flagging of data changes</p> <p>Retrieval of like images despite angle of look and shades of gray differences</p> <p>Understanding of numeric variations</p>	<p>Database construction and management</p> <p>Free form database construction</p> <p>Automated database maintenance and updating</p> <p>Automated verification and cleansing of data</p> <p>Automated text extraction</p> <p>Automated tagging of data elements with level of classification and source</p> <p>Fully integrated text and images</p> <p>Automated and ad hoc hot links easily applied</p> <p>Automated records management</p>

and equivalents	Individual entry protocols for voice and video
<p>Data collection and exploitation</p> <p>Desktop publishing</p> <p>Graphics and briefing aids</p> <p>Global electronic mail</p> <p>Graphical visualization of trends and linkages</p> <p>Menu of modeling and simulation programs</p> <p>Automated statistical analysis</p> <p>Expert pre-screening of indicators and warning</p> <p>Automated flagging of "hot" words and changes in content over time</p> <p>Digital map overlays and grid coordinate input</p> <p>Tailored no-notice map productions to the 1:50,000 level</p> <p>Automated overlay maintenance</p>	<p>Knowledge base construction and management</p> <p>Menu driven access to previous queries</p> <p>Automated repeat queries</p> <p>Menu driven flagging of key words, profile extensions</p> <p>Gradual automated and user-assisted development of key links and concepts</p>
<p>"Intelligence" collection management</p> <p>Automated collection asset inventory and status</p> <p>Automated matching of assets and requirements</p> <p>Automated "tasker"</p> <p>Automated tracking of satisfaction/tickler</p> <p>"Alternative collection strategies" generation</p> <p>Raw/finished collection evaluation toolkit</p>	<p>Administrative and security management</p> <p>Classified documents control/bar coding</p> <p>Electronic "marking" of classification by word</p> <p>Automated sanitization to any level</p> <p>Automated comparison of like/unlike reports</p> <p>Quick search OOB and terminology library</p> <p>Automation of all forms and reports</p> <p>Automated name traces on refugees and prisoners for any location</p> <p>Automated access/query audit trail</p> <p>Automated virus detection &amp; eradication</p> <p>Smart in-boxes (prioritizing and screening)</p> <p>Instant retrieval of any order, manual, handbook, or other official document</p> <p>Instant retrieval of any contingency plan to which the individual is a party</p>

Figure 5: Generic "All-Source Fusion" Workstation Requirements

Above have been a few illustrative examples of generic requirements, which should be part of joint government-corporate efforts to establish an international information technology standard, which contributes to individual productivity: The technologists will be quick to say "we can do that", but there are two realities that continue to escape them:

Human productivity and human nature cannot afford to learn a different application for each function and task. These are basic functions and tasks, which must be integrated and intuitive.

Crazy things happen when multi-media and multi-lingual data is needed which can only be obtained from multiple remote sources. No technology should be considered acceptable until it has been fully tested against the real-world data sources and real-world data processing needs of the end-user.

It is essential, therefore, that *policymakers* present a united front, across organizational and even national boundaries, with respect to the generic functional requirements for the single most important tool in the arsenal of the diplomat: the electronic information machine.

Now with respect to external access, and the creation of an architecture through which policymakers can obtain open source intelligence from the private sector, the following two illustrations outline the core ideas for the "information merchant bank" which has been established by the author in prototype.



Figure 5: Concept for Providing Four Levels of Open Source Information Service

**Early Bird (Periodic Awareness Service).** The lowest level of service is the daily *Early Bird* which builds on a quality process such as that offered by Individual, Inc., and provides to each individual policymaker (or supporting staff employee) a one page digest of highly focused current news—each entry comes with a route to obtaining the full text document.

**Help Desk (Online Search & Retrieval).** The next level of service, the Help Desk, provides rapid response search and retrieval services which can access the Internet, all major commercial online services including international and foreign language online services as well as international electronic databases that are not necessarily "online" but can be exploited remotely, and hard-copy references including general literature such as is available in a major library.

**Primary Research (Experts on Demand).** At the third level, even more expertise can be brought to bear on a policymaker's problem by systematically identifying and then contracting with individual experts who can bring to bear decades of experience and immediate access to all manner of electronic and hard copy sources (as well as their own network of experts and assistants). The economic benefits of out-sourcing decision support to such experts cannot be understated—this essentially allows the policymaker to harness expertise that has been maintained at someone else's expense, and that has proven itself in the marketplace through peer citation and public success. Oxford Analytica, which uses the Dons of Oxford University as a *de facto* "Intelligence Council", is the only organization of its kind, and an integral part of any comprehensive effort to take advantage of the knowledge available in the private sector.

**Strategic Forecasting (Including Technology Forecasting).** Finally, at the fourth level, strategic studies and forecasts, including forecasts of scientific and technical trends and opportunities, can be obtained by using the capabilities of the Institute of Scientific Information (ISI). This unique organization is the sole source in the world of both citation analysis data, which covers all significant peer-reviewed journals in the

world (i.e. it is international and multi-lingual) as well as essential technology for mapping specific disciplines and identifying key individuals and centers of expertise. In combination with a wide range of other open sources, systems, and services, relatively low-cost strategic forecasts can be developed.

Any organization can establish its own clearinghouse for gaining access to external expertise and knowledge. It may not be as effective as using a "virtual" intelligence center provided by a global leader in open source exploitation, but it will assuredly improve-significantly improve-day to day decision support and hence contribute to the effectiveness of the organization.

Below is an illustration of a basic internal clearinghouse, and a brief description of its core functions.

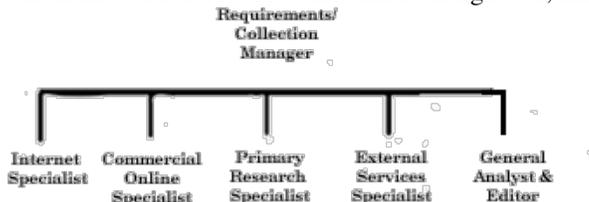


Figure 8: Generic Concept for Open Source Intelligence Support Cell

The above "cell" is scalable, but the key idea is to avoid at all costs the creation of a centralized unit with increasing numbers of employees which attempts to actually do the research and develop the intelligence itself. Instead, the focus for *each* of the specialists must be on "knowing who knows"

**The Internet specialist** keeps track of external Internet experts who are also subject-matter experts, for instance in regional, scientific, or military domains, and who can be called upon to carry out specific searches of the Internet. This specialist also monitors the development of new Internet technologies.

**The commercial online specialist** must understand in strategic terms the relative utility and price value of the various commercial online offerings, and focuses on retaining the appropriate information broker or brokers, each with the necessary expertise at particular online services, as well as a complementary knowledge of the language and /or foreign databases as well as the subject matter area.

**The primary research specialist** is expert at using a combination of citation analysis, association and other directories, and direct calling to rapidly get answers to questions which cannot be addressed through accessing published information, but rather require either access to "gray literature" that is legally available but only if you know where to go for it, or to a human expert who can construct the answer in real time by drawing on their historical knowledge and access to various sources, including human sources.

**The external services specialist** (some might wish to distinguish between an external systems specialist and an external services specialist) is a master of the marketplace and follows all of the niche providers who offer narrowly focused technologies (e.g. search & retrieval technologies, visualization technologies) or services. Below are some of the standard niche services that are common to the private sector:

Open Source Examples	Open System Examples	Open Service Examples
Current Awareness	Internet Search Tools	Commercial Online Search & Retrieval
Current Contents	Data Entry Tools	Foreign Language Media Monitoring

Subject-Matter Clearinghouses (Univers.)	Database Construction and Management Tools	Human Document Abstracting and Indexing
Conference Proceedings and Papers	Data Retrieval, Routing, and Records Management	Document Translation
Direct Access to Commercial Online	Automated Document Abstracting and Indexing	Gray Literature Discovery and Retrieval
Contextual Awareness/ Cultural Orientation	Automated Document Translation	Experts on Demand
Document Acquisition	Knowledge-Base Construction & Mgmt.	Primary Research (Telephone Surveys)
Subject-Matter Commercial Databases	Data Mining and Visualization Tools	Private Investigation and Direct Debriefings
Risk Assessment Reports	Desktop Publishing Tools	Market Research
Expert and Association Directories	Multi-Media Communications Tools	Strategic Literature and Technology Forecasting
Photographic Archives	Digital Imagery Processing	Hard-Copy Global Map and Chart Procurement
Digital Data Archives	Electronic Security and Administration Tools	Commercial Imagery and Map Production

Figure 7: Standard Niche Capabilities Offered Within the Private Sector

"Market research" and "studies & analysis" are generic categories where in many cases the customer cannot rely on the provider. In general, providers of such services who have major investments in permanent

personnel will *not* take the trouble to systematically identify world-class experts or fully survey external online and hard copy sources. It is an unfortunate reality that such organizations are constantly seeking to assign existing employees, whether or not they are fully qualified to address the specific inquiry, and to avoid paying for direct support from niche providers such as those who specialize in specific languages, citation analysis, patent records search, etcetera.

Information technology continues to offer the policymaker significant opportunities for acquiring and managing knowledge with which to avoid conflicts and resolve conflicts, as well as to identify and exploit opportunities for mutual peaceful advantage, but it will not be part of the solution until the policymaker recognizes that in the age of information, the management of information technology is an inherent function of command, and not something which can be delegated to technologists.

It is also critical that the policymaker focus on content and access to external expertise and multi-lingual data as well as value-added services, and not on internal information handling systems which tend to require more effort to "feed" than they return in value-added.

In the age of information, the cost of communications and computers (hardware and software) has already declined dramatically. Now the cost of content is leveling off and is about to begin declining. The major added value in the next two decades-and information technology has an important but not an exclusive role to play in delivering this added value-will come from:

- 
- **Discovery.** Policymakers have power and they should spend their time reflecting and deciding when they are not in negotiation and in face to face communication with their counterparts. It is for the "virtual intelligence community" to meet the policymakers needs for discovering as much of the raw information as is necessary to meet the policymakers needs for "just enough just in time" intelligence.
- **Discrimination.** A major value-added function is that of discriminating between valid and invalid information, through a constant process of source validation, generally a labor-intensive process requiring genuine human expertise as well as new developments in automated understanding. A cost element can also be provided here, by giving the customer the benefits of superior knowledge in selecting sources of equal content but lower prices.
- **Distillation.** This is the essence of "intelligence" in that it combines research judgements which first discover and discriminate, and then it adds expert subject matter knowledge to distill the broader effort into "just enough" intelligence-intelligence being information which is tailored to the needs of the policymaker and tightly focused on helping the policymaker with a specific decision at a specific time and place.
- **Dissemination.** Often the timing, length, and even the format of the delivered product can be decisive in determining whether the intelligence contained in the document (or oral presentation, or video, or electronic mail, or whatever) is received by the intended policymaker, absorbed, and compelling enough to support action. There is far more to dissemination than simple delivery.

The above is not intended to make a case for the use of open sources from the private sector to the exclusion of either unclassified information or classified information from government sources. Indeed, the ideal situation emerges when both the policymaker and the intelligence community use open sources to the fullest extent possible, but with intelligence methods applied to produce open source intelligence, *then* task the classified systems for such information as is truly critical, and finally utilize open sources to protect classified findings but inform those who require information support but to whom classified information

cannot be disclosed.

## Part IV: Strategic Information Management for Global Peacekeeping

The private sector offers the policymaker an extraordinary range of world-class expertise at very low cost, and with the ability to create new knowledge on demand. In most cases having to do with Third World conflicts, traditionally very low priorities for classified intelligence capabilities, the private sector is the essential source for expertise needed by the policymaker. At the same time, the policymaker can acquire a new appreciation for information as a "munition" or a means by which to alter the balance of power in a conflict through an alteration of the balance of information. A new theory is presented, the theory of "information peacekeeping", whose elements are (unclassified) intelligence, information technology ("tools for truth"), and electronic home defense. The article concludes that the private sector can be harnessed by the policymaker in a non-intrusive way, but that a national information strategy is required if the policymaker is to be effective in fully integrating and exploiting classified and unclassified government information as well as private sector information. Given a national information strategy, the policy maker can create a "virtual intelligence community" and utilize "information peacekeeping" as a means for the conduct of virtual diplomacy.

In this final part of the article we examine three elements which, taken together, can help avoid and resolve conflicts while significantly increasing the productivity and effectiveness of those practicing "virtual diplomacy":

Distributed Expertise in the Private Sector-The Information Continuum

Information Peacekeeping and "Tools for Truth"

Information Strategy as the Enabler of Virtual Diplomacy

Distributed Expertise in the Private Sector-The Information Continuum.

The following illustrates the "information continuum" which exists today, the vast majority of it in the private sector:

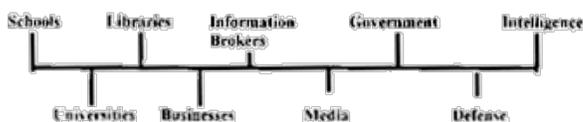


Figure 8: The Information Continuum

In contemplating this continuum, the policymaker should consider the following key findings:

The expertise contained within each of the sectors is created and maintained at someone else's expense.

The expertise which is maintained in these other sectors is constantly subject to the test of market forces, and tends to be more current with respect to both sources and methods than the government's archives and analysts.

The cost of this expertise, when the policymaker is able to surmount security and procurement obstacles, is on the order of \$10,000 for a world-class report which is concise and actionable and delivered overnight, inclusive of the cost of identifying and validating the best choice of expert.

Such published information as is available to the policymaker through either online retrieval or hardcopy

document retrieval represents less than 20% and more often less than 10% of what is actually known by the individual experts.

The most significant deficiency in national intelligence today as it pertains to providing the policymaker with just enough, just in time "intelligence", is the lack of direct access to the expertise available in the private sector.

There are many examples of worthy private sector sources and capabilities, which can be harnessed to meet the needs of the policy maker, but for the sake of this article, a practical case study pertinent to conflict resolution, will be reported.

On the afternoon of 3 August 1995, a Thursday, the author was testifying to the Commission on Intelligence regarding the importance of dramatically improving government access to open sources. At the end of the day, at 1700, the author was invited to execute a benchmark exercise in which the U.S. Intelligence Community and the author would simultaneously seek to provide the Commission with information about the chosen target, Burundi.

By 1000 the morning of 7 August 1995, a Monday, the following was delivered to the Commission offices via overnight mail:

**From Oxford Analytica**, a series of two-page executive reports drafted for their global clients at the Chief Executive Officer level, outlining the political and economic ramifications of the Burundi situation;

**From Jane's Information Group**, a map of Burundi showing the tribal areas of influence; a one page order of battle for each tribe; and a volume of one-paragraph summaries with citations for all articles about Burundi published in the past couple of years in *Jane's Intelligence Review*, *International Defense Review*, and *Jane's Defense Weekly*.

**From LEXIS-NEXIS**, a listing of the top journalists in the world whose by-line reporting on Burundi suggested their intimate familiarity with the situation;

**From the Institute of Scientific Information (ISI)** in Philadelphia, a listing of the top academics in the world publishing on the Burundi situation, together with contact information;

**From East View Publications in Minneapolis**, a listing of all immediately available "Soviet" military topographic maps for Burundi, at the 1:100,000 level.

**From SPOT Image Corporation (USA)**, it was determined that SPOT could provide digital imagery for 100% of Burundi, cloud-free and less than three years old, at a ten meter resolution adequate for creating military maps with contour lines at the 1:50,000 level as well as precision-munitions guidance packages and nape of the earth interactive aviation and ground mission rehearsal simulation packages.

The above effort has received wide recognition among those who are responsible for oversight of the U.S. Intelligence Community, and was described by one very senior Hill staff manager as "John Henry against the steel hammer-only John Henry won." In fact, it is very important to stress again and again that open sources are *not* a substitute for spies and satellites (the author has been the first and worked with the second), but rather that both common sense and fiscal realities suggest that it is imperative that the policymaker be able to exploit open sources to the fullest in their public diplomacy, military acquisition, and economic competitiveness roles, while relying on classified intelligence-classified intelligence presented in the *context* of open sources-for those unique insights and details which cannot be obtained through other means, and which in fact are demonstrably so precious as to warrant the risk and cost of espionage.

**Information Peacekeeping and "Tools for Truth"**. As policymakers contemplate the advantages of virtual diplomacy and the potential of information technology, they may wish to absorb the implications of a new theory of information peacekeeping, and the value of "tools for truth".

Information Peacekeeping is the active exploitation of information and information technology in order to modify the balance of power between specific individuals and groups so as to achieve one's policy objectives. The three elements of information peacekeeping, in order of priority, are intelligence (providing useful actionable information); information technology (providing "tools for truth" which afford the recipient access to international information and the ability to communicate with others); and electronic home defense, a strictly defensive aspect of information warfare.

Information peacekeeping is *not*:

the application of information technology in support of conventional military peacekeeping operations, or in support of coalition humanitarian assistance operations;

the development and execution of traditional psychological operations which focus on manipulating perceptions and imposing strategic deceptions;

covert action media operations, covert agent of influence operations, or covert action paramilitary operations; nor

clandestine human intelligence.

Information peacekeeping "gray areas" exist.

Information peacekeeping may require the clandestine delivery of classified or open source intelligence, or the covert delivery of "tools for truth" (cellular phones, fax machines, personal computers and software for accessing and contributing to the Internet).

Information peacekeeping may require the covert delivery of assistance in electronic home defense, or selective information warfare operations (either overt or covert) in order to "level the playing field" between emerging democratic and popular nodes, and their oppressive opponents.

On balance, information peacekeeping is by its nature most powerful and most effective when it relies exclusively on open sources of intelligence and on overt action, and when it is therefore incontestably legal and ethical under all applicable rules of law including host country and non-Western cultural and religious rules of law.

Some general principles of information peacekeeping, which build on the information provided in the first three sections of this article:

Policy options have to start "here" at home, during violent "peace", and now.

Information peacekeeping is the ultimate global presence.

Information peacekeeping is the *first* policy option-both to ensure that the policymaker has a full knowledge of the situation, and to impact constructively on those we seek to influence.

We need to develop an information peacekeeping "order of battle" with related tables of organization and equipment-much of this can be "virtual" and rely on private sector providers of information and information technology who are mobilized "just in time".

Information peacekeeping is the operational dimension of a broader approach to national intelligence.

The nature of global security and the ease of movement of transnational criminal and other rogue elements requires the inseparable integration of law enforcement, military, and civilian agencies as well as all elements of national intelligence into a larger global information architecture.

Information is the ultimate *countervailing force* against the emerging threats, and the most cost-effective

means of devising diplomatic and other responses intended to avoid or resolve conflicts.

At least 80% of the information the policymaker needs to conduct information peacekeeping operations is not controlled by the government-"knowing who knows" and the creation of management, technical, security, and procurement architectures which permit harnessing distributed intelligence, is the emerging new source of national power.

Because the policymaker is inundated with contradictory information lacking methodical evaluation, a critical priority must be the transfer of proven methods of classified intelligence analysis, to the world of unclassified information.

Unclassified information is critical to converting policy minds and winning public hearts. The policy maker *can* succeed without classified information but the policy maker *cannot* succeed without a mastery of unclassified information.

Multi-channel delivery of "truth" is the SIOP of the information age

Information peacemaking is an information-intensive process with both mass and niche audiences-information peacekeeping is not a low-cost alternative to traditional warfare, but it *is* less expensive.

The information "center of gravity" will vary from conflict to conflict, from level to level, and from dimension to dimension. The greatest challenge for the policymaker will be to manage a national intelligence architecture, which can rapidly identify the information center of gravity, prepare the information "battlefield", and deliver the appropriate (non-lethal) information "munitions" to carry the day.

## INTELLIGENCE

### INFORMATION TECHNOLOGY ELECTRONIC HOME DEFENSE

#### Figure 9: Integrated Elements of Information Peacekeeping

Information peacekeeping starts and succeeds with *intelligence*-accurate and comprehensive analyzed information tailored to the needs of the policymaker and useful to the participants in the emerging or on-going conflict.

Intelligence, while always the fundamental aspect of "information peacekeeping", must be developed in full consonance with both an information architecture capable of discovering, discriminating, distilling, and disseminating multi-lingual and multi-media information; and with an electronic home defense capability that is the cyberspace equivalent of peaceful resistance and protection through preparedness.

Information peacekeeping operations cannot be successful without a very strong multi-lingual capability and a very strong cultural intelligence element.

The objective of information peacekeeping is to alter the knowledge balance of power and to substitute information and dialogue for violence and extortion.

Information peacekeeping requires a national information strategy and the deliberate development of a national

information architecture fully integrated into a global information architecture of knowledge.

**Information Strategy as the Enabler of Virtual Diplomacy.** There are four elements to a national information strategy, which can empower those who would seek to practice virtual diplomacy and avoid or resolve conflicts:

**Connectivity.** Lest we become too complacent about connectivity as "virtual" strategy, let us paraphrase the earlier observation of the (then) Commandant of the Marine Corps: "Connectivity without content is *noise*; content without connectivity is *irrelevant*." The National Information Infrastructure (NII) and Global Information Infrastructure (GII) are brilliant initiatives worthy of a great nation, but they are seriously flawed in that they do not address issues of content and especially of how the policymaker can use the NII and GII to nurture distributed centers of expertise and fully integrate, in real time, the classified intelligence available from selected elements of the government, unclassified government information, and the often more accurate, comprehensive, and lower-cost information available from the private sector.

**Content.** The private sector will not open itself to control or regulation by the intelligence community, nor will it cooperate with any initiative, which seeks to impose government oversight upon private sector expertise and data. It will, however, welcome government subsidization of the marginal cost of providing increased public access to its expertise, in the same fashion that the National Science Foundation (NSF) nurtures selected scientific & technical initiatives. A National Knowledge Foundation (NKF), funded with just \$1 billion a year by which to nurture distributed centers of subject-matter expertise which permit increased public access to their knowledge, could yield enormous productivity gains in both the private and public sectors. International agreements to implement a Global Information Management (GIM) burden-sharing agreement could radically reduce the cost of information for Third World and other policymakers, and begin the process of creating an "information commons" which can support virtual diplomacy.

**Coordination.** There is an urgent need for voluntary coordination in the arena of standards, of content acquisition and development, and of resource management. Billions of dollars a year are being wasted in the United States alone, simply for lack of coordination across industrial sectors and organizations.

**Communications and Computing Security.** The vulnerabilities of our financial, communications, power, and transportation infrastructures, all with very heavy computational aspects which are easily attacked by both physical and electronic means, are just now emerging into the public eye, despite a decade of effort by spirited citizen-leaders such as Winn Schwartau. The intelligence community continues to classify the electronic threat as well as the economic espionage threat, and Congress continues to ignore the need for legislation defining "due diligence" in the electronic arena.

There are many other comments that could be made in conclusion, but at this point, if the four parts of the article have been successful, a simple summary should suffice:

We need to know about our world in terms and by means that impact on our day-to-day decision making;

The classified intelligence community as it stands today is not able to meet the needs of the policy makers for real-world intelligence that is timely, accurate, and deep in understanding;

Neither the intelligence community nor the policymaker have adequate access to the wealth of information available in the private sector;

A national information strategy can resolve these deficiencies and make the contributions of the intelligence community much more important in the context of unclassified information properly analyzed, and it can also empower the policymaker by making possible the execution of a new form of global power, information peacekeeping.

The really good news is that in comparison with the funding of military systems, contingency operations, disaster relief, and many others aspects of government, a national information strategy-and the resulting

ability to create a virtual intelligence community and to conduct information peacekeeping operations-is available today at a fraction of the cost of any alternative program. One billion dollars per year for a National Knowledge Foundation, and no cost at all for a change in approach to information management-this is easily affordable in the context of \$3 billion per year in savings from improvements in the management of unclassified information technology, and \$10 billion per year in savings from refocusing classified information technology toward "the hard stuff". We *can* create a Smart Nation able to practice "information peacekeeping".

- **"To worry about war or anti-war in the future without rethinking intelligence and seeing how it fits into the concept of knowledge strategy is an exercise in futility. The restructuring and reconceptualization of intelligence-and military intelligence as part of it-is a step toward the formulation of knowledge strategies needed either to fight or forestall the wars of tomorrow."**

Alvin and Heidi Toffler, *WAR AND ANTI-WAR: Survival at the Dawn of the 21<sup>st</sup> Century* (Little Brown, 1993)

---

The views expressed in this report do not necessarily reflect views of the United States Institute of Peace, which does not advocate particular policies.

*This paper was prepared for the [Virtual Diplomacy](#) conference hosted by [United States Institute of Peace](#) in Washington, D.C. on April 1 and 2, 1997.*

[Back to Top](#)

---

[Home](#) | [Jobs](#) | [FAQs](#) | [Contact Us](#) | [Directions](#) | [Privacy Policy](#) | [Site Map](#)

---

United States Institute of Peace -- 1200 17th Street NW -- Washington, DC 20036  
(202) 457-1700 (phone) -- (202) 429-6063 (fax)  
[Send Feedback](#)