Document generated on 04/18/2024 8:28 p.m.

Journal of Conflict Studies

Virtual Intelligence: Conflict Avoidance and Resolution Through Information Peacekeeping

Robert David Steele

Volume 19, Number 1, Spring 1999

URI: https://id.erudit.org/iderudit/jcs19_01art04

See table of contents

Publisher(s)

The University of New Brunswick

ISSN

1198-8614 (print)
1715-5673 (digital)

Explore this journal

Cite this article

Steele, R. D. (1999). Virtual Intelligence: Conflict Avoidance and Resolution Through Information Peacekeeping. *Journal of Conflict Studies*, *19*(1), 69–105.

All rights reserved © Centre for Conflict Studies, UNB, 1999

This document is protected by copyright law. Use of the services of Érudit (including reproduction) is subject to its terms and conditions, which can be viewed online.

https://apropos.erudit.org/en/users/policy-on-use/

érudit

This article is disseminated and preserved by Érudit.

Érudit is a non-profit inter-university consortium of the Université de Montréal, Université Laval, and the Université du Québec à Montréal. Its mission is to promote and disseminate research.

https://www.erudit.org/en/

Virtual Intelligence: Conflict Avoidance and Resolution Through Information Peacekeeping

by
Robert David Steele

INTRODUCTION

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 is the ever-widening chasm between policy makers 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 that focuses on content as well as connectivity and enables policy makers to draw upon the expertise available in the private sector. The United States requires 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: indeed, virtual intelligence *is* virtual diplomacy.

This article explains the concepts of virtual intelligence and information peacekeeping in four parts. Part 1 discusses the nature of conflict as an analysis problem; what do we need to know and how? Part 2 reviews a number of acknowledged deficiencies of the classified intelligence community and identifies some inherent related problems in government mis-management of unclassified information. Part 3 examines the strengths and weaknesses of information technology as currently developed and used by governments and corporations why we are substituting technology for thinking but also, how technology can help us think and gain access to external expertise. Finally, Part 4 discusses the information archipelago (comprised largely of private sector communities 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. This 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 1: WHAT WE NEED TO KNOW AND HOW?

The policy maker needs an intelligence support system that is directly related to their daily schedule, that provides just enough intelligence just in time, at the lowest possible level of classification, and that 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 policy maker with both strategic generalizations and complete cultural, technological and geographical 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 policy maker 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 that has been discovered, discriminated, distilled, and disseminated in a form tailored to the needs of a specific policy maker/commander at a specific time and place. Intelligence most often is not classified and its utility tends to decrease dramatically with every increase in its level of classification.1 In today's global environment, intelligence that can be shared and that does not compromise the political standing of the sponsors of the intelligence by relying on covert means is vital.2

INNOVATION: 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 customers with an electronic means of indicating whether they actually read the report and of grading the report (at its various levels) in real time.

Just Enough

The policy maker/commander does not have the time or the inclination to digest vast quantities of information. The successful analyst supporting the leader will have gained their trust and understanding and will provide "just enough" intelligence to permit the leader to grasp the essence of the value-added information (i.e., insights he/she did not already have) and to provide the analyst with guidance if additional detail or other related analytical paths are to be pursued.

INNOVATION: Require that intelligence be delivered via web-like applications that begin with a paragraph and allow the policy maker to access 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. It can be applied on behalf of the large number of policy makers who require hard-copy products, by automating the production process so that four levels of detail are provided.

Just in Time[3]

Twelve month research plans and eighteen month editing cycles have made most "intelligence" irrelevant to the day-to day needs of the readers who require intelligence that is pertinent to the decisions they are making that very day (including decisions that set in motion longer terms endeavors by others).

INNOVATION: To the extent that the leader is willing, ensure that their daily agenda is electronically available to all analysts supporting them, kept up to date and used as the electronic "hot link" for providing intelligence support. As the policy maker looks at their daily agenda on their screen, they should see a little "icon" that says "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 21st century, the acme of skill for the master analyst will be the ability to put a policy maker with a "hot" question in direct contact with a world-class expert (generally in the private sector) who in real time can provide him/her with an informed judgement that is tailored to his/her precise nuances of concern.[4]

INNOVATION: Using Web technology, establish a secure "virtual intelligence community" directory, which would be updated constantly by the Institute of Scientific Information and would permit any analyst or policy maker to identify quickly and exploit world-class experts on any subject.[5]

Earth Map

The leaders, their 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 for decision-making, it is vital as the foundation for fusing information from various collection disciplines (imagery, signals, human) and for automating the visualization of information in the aggregate. The United States has less than 10 percent 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.[6] In both Somalia and Burundi, the next best alternatives to tourist maps are previously classified Soviet military topographic maps at the 1:100,00 level, only recently made available through a US company, East View Publications.

INNOVATION: Earmark $250 million year to the Department of State to procure commercial imagery sources and related processing services to support both peacekeeping initiatives and EARTHMAP Report requirements of other civilian agencies. Those 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 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 the area.

Strategic Generalizations

The policy maker requires strategic generalizations with which to plan and direct operations. However, for a lack of a model of analysis which requires them to address the peacekeeping environment in a comprehensive manner which readily brings out useful generalizations, analysts and their managers too frequently inundate the policy maker with thousands of "current intelligence" updates and also exaggerate the threat. In 1989, after the Marine Corps Intelligence Center (now Activity, MCIA) was established, a review of available Central Intelligence Agency (CIA) and Defense Intelligence Agency (DIA) production found that they could provide 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 military capability being considered and the pertaining civil and geographical factors in the area of operations. Below is a high-level view of the model.7

Figure 1

Two examples of this model's utility are offered because its implications are so important to policy makers dealing with complex conflict situations. In a test case discussed with the appropriate analysts from all of the major US intelligence agencies, the MCIA 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 most powerful main battle tanks other than American), 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 fell 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*. The MCIA considered this very significant to the perspective of the policy maker or commander making decisions about overall structure of the force to be deployed to this region, even in the absence of related information about civil and geographic features.

A second example illustrates the importance of civil and geographic factors to the overall analysis of any peacekeeping situation or related acquisition and employment decisions. The Commandant of the Marine Corps asked the MCIA to evaluate the Corps requirement for a follow-on procurement of the M1A1 tank. The MCIA examined civil and geographical factors for the sixty-nine countries (now eighty) that comprised the expeditionary environment and discovered the following "strategic generalizations":8

Intervisibility (Line of Sight Ranges): 91 percent 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 percent of the countries offered *zero* cross-country mobility; the terrain would require all mobility platforms to use normal roads. Most of their bridges have loading limitations of 30 tons (+/-), making the M1A1's 70 ton weight a distinct liability; and,

Ports: 50 percent of the countries did not have a port usable by a US Navy or Maritime Pre-positioned Force (MPF) ship. They lacked adequate depth, turning radius and/or piers and cranes. This means that the M1A1 would have to be off-loaded in mid-stream, using scarce and often inadequate landing craft.

A similarly strategic observation subsequently was made with respect to aircraft, which are designed by the US Navy for the US Marine Corps based on a standard aviation day that is warm (around 65°F) and with average humidity. In fact, the Marine Corps aviation day is in fact *hot* (routinely over 80°F) with very high humidity. Consequently, Marine Corps aviation can carry only half as much only half as far as the manual 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 geographical realities. This is of special concern with respect to Non-combatant Evacuation Operations. Further, in this regard, the MCIA also discovered that: most US 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 US Navy five-inch gun with their existing shore batteries and; the US allies are completely lacking in digital imagery and 1:50,000 combat charts for operations in 90 percent of the world,9 as well as being 200 ship-years behind in shallow water (100 fathom or less) hydrography.

Why is this so important? The fact is that policy makers are often ignorant of the realities of the military, civil, and geographic elements in relation to one another; this ignorance and the level of analysis lead to woefully inadequate estimates of what it will take to achieve stated objectives. At the same time, the military and their policy masters are largely uninformed as to the "intangible" aspect of the situation, and the military itself is generally is not trained, equipped and organized for operations which require that they deal with people rather than kill them.10 One solution may be to post the MCIA study - on a site where leaders can be sure to see it.

Multi-Dimensional

The policy maker is poorly served when analysts focus only on the political-legal situation, or the military situation, or on the economic situation. Every emerging and on-going conflict has a multi-dimensional nature and must be understood across a spectrum that includes sociological, economic, ideological, cultural , technological, demographic, natural, and geographical conditions. At the same time, culturally astute experts must

study the aspects of human development and the local psychology and these informed judgements must be factored into the decision-making process. However, the average analyst is pre-occupied with cutting and pasting miscellaneous "current facts" from classified and other government sources, and lacks access to sources of cultural and other forms of "intangible" intelligence as well as access to tools for visualizing complex integrated problem sets. Working from a generic requirements plan, rarely, if ever, could that analyst provide the policy maker with insights into the multi-dimensional nature of a conflict and consequently unanticipated consequences of revolutionary change in the non-traditional dimensions such as the ideo-cultural or techno-demographic.

For this reason, it is essential that we have two required analysis models: the first focusing on the levels of analysis and the inter-relationship between military, civil and geographic sources of national power; the second focusing on the dimensions of national power: political-legal; socio-economic; ideo-cultural; techno-demographic and natural-geographic. Figure 2 offers a matrix of the kinds "indications & warnings" country study and related politics should take into account.11

INNOVATION: 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" and also highly fragmented Army *Country Studies*. Then develop a Web-based network of sites and publications organized by country and within country so as to allow any policy maker 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. Using 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 21st century. Both merit brief discussion, because the lack of knowledge among policy makers and the mind-set inertia of the analysts supporting them suggest that we are not making significant changes in the ways 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 with since the end of World War II and the emerging threats which we are not trained, equipped, or organized to identify and evaluate.12 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. Consider figure 3 that follows.

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, information vandals, and criminal hackers stealing what they can from an unwitting world of nations, corporations, and citizens. They practice information warfare, have knowledge as their source of power, and they rely on cyber-stealth and database targeting for their effect.

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

Low-Tech Brains are the "wild card" of history and are presented by religious fundamentalists and cults (which do not merit religious status). They practice "holy war," have ideology as their source of power, and rely on mental stealth and mass targeting for their effect.

INNOVATION: Establish an inter-agency working group, with extensive representation from the private sector and especially including law enforcement, hackers, and non-governmental organization analysts. Have them 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, as well as sermons and distributed audio-visual messages to "the faithful" that are not properly monitored by the Foreign Broadcasting Information Service (FBIS).

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. It is imposing on our government policy organizations and on our national and law enforcement intelligence communities a dangerous and probably catastrophic barrier to the development of seamless lines of communication and shared knowledge. This includes knowledge about: the movements of transnational criminal gangs and terrorist organizations, major religious as well as cult organizations; alien-smuggling operations; and individuals participating in economic espionage, information terrorism and/or information vandalism, in association with international partners, be they governments, corporations, gangs, or other individuals. Consider the following illustration (figure 4)13

This chart has two meanings with regard to how we devise policy and execute operations. First, it demonstrates the urgency of creating a seamless architecture for linking policy makers, 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. 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 will not have the luxury of time to recognize threats gradually, devise means of monitoring them, and finally come to consensus on means dealing with them, after which the means can be implemented gradually. 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 to be able to respond rapidly to threats beyond the *ken* of the conventional government policy maker, 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 opportunities. Each is much more subtle, more diffuse, and obtuse than the traditional conventional threat the US has grown to rely on for its feeling of security (that we understand our world). As will be shown in the next section, the US 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 need of international policy makers and that have the added advantage of avoiding the constraints associated with classified information.

PART 2: WHY DON'T WE KNOW WHAT WE NEED TO KNOW?

The American policy maker today suffers from a triple liability. First, the intelligence community is optimized for processing secrets out of context (without adequate access to open and especially multi-lingual sources of information). Second, the government's information handling system is unable to deal with the flood of unfiltered and unanalyzed information directed at the policy maker from hundreds of international advocacy sources all pressing their own agenda. Finally, the policy process is inherently focused on domestic political decision criteria, which are acted upon with little time for reflection.14

No person who really understand 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 predominately on open sources. Unfortunately, the allure of clandestine operations against the Soviet Union and then the failure of those operations, led the United States to invest heavily in narrowly focused satellite technology, to the detriment of both its clandestine human intelligence collection capability and its severely degraded analysis capability.15 In general terms, the US intelligence community fails to meet the needs of the policy makers because, first, 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.16 Second, it is extremely dependent on classified overhead satellite collection assets,17 and is severely lacking in commensurate investments in commercial imagery and signals collection, data processing, human clandestine collection and human analysis capabilities.18 Third, by inclination in terms of management and culture and by design in terms of budgets and technology, it is completely isolated from the larger worlds of government and private sector information and intelligence. Fourth, it persists in using a priorities-driven requirements system in which repetitive collection against generally 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. Finally, it lacks both a model and a process of analysis.

In systematic terms, in relation to the four major functions of intelligence and in relation to the four major consumer groups, the US intelligence community is not trained, equipped and organized to be effective against the complex threats and opportunities which face US policy makers and their global partners today. The vaunted individual disciplines of classified intelligence are intended to provide policy makers with "plans and intentions" intelligence, as well as a full gamut of encyclopedic intelligence, current intelligence, indications and warning, estimates, military intelligence, and scientific and technical intelligence.19 Figure 5 identifies explicitly the major deficiencies of the US intelligence community in relation to the four levels of consumer and the four major functions. Relevant to the figure are the following summaries of unclassified extracts from the evaluative comments that received policy and security approval within the Marine Corps.20

General Military Intelligence (GMI) Production. More attention should be devoted to integrating intelligence about operational geography and civil factors pertinent to military operations into overall estimates.

Scientific & Technical Intelligence (S&TI) Production. Military planners and programmers would benefit from expanded analysis of the S & TI function to include: Third World arms production programs, weapons sales, and thefts and technology transfer. There is a need to improve integration of both HUMINT reporting and annotated imagery into S&TI production. S&TI databases on the Third World appear to be inadequate.

Indications & Warnings (I&W). Many non-military crises require a commitment of military resources for stability or humanitarian reasons. There is concern about absence of an estimative methodology and dedicated resources for anticipating such crises. The community must have a "peacetime engagement" I&W capability, together with a capability to produce estimates relevant to national security planning and programming for Third World stability operations.

Human Intelligence (HUMINT). The most fundamental concern is that the existing intelligence capability is simply not able to meet the need for military and non-military plans and intentions. Nor can it provide contingency support and stay-behind ground resources reconnaissance and support assets, especially in the Third World.

Signals Intelligence (SIGINT). The proliferation of commercial technology, the reduction of 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 received under the defense draw-down. The SIGINT community is beset by other challenges, including a lack of qualified linguists for many lower priority (but high crisis probability) languages.21

Imagery Intelligence (IMINT). The emergence of multi-spectral imagery and its commercial availability, together with possible economies achievable by modifying airborne targeting radar, offer innovative alternatives for meeting some of the most pressing requirements.

Collection Management. The national intelligence community must strive to establish a national requirement 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.

Automated Data Processing (ADP) and Intelligence Communications. The intelligence community must have global data-driven C^4I^2 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 requirements for intelligence and information sharing with US law enforcement, foreign military, and non-governmental humanitarian organizations.

Processing and Dissemination. Processing and dissemination management 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 finally have made product and system two sides of the same coin; planning processes in these areas must be integrated.

Intelligence Training. There should be more emphasis on the development of advanced analysis methods and tools throughout the community and of a means of exporting these methods and tools to all analysts. The community needs to do a better job of educating non-intelligence professionals regarding all aspects of intelligence, including how to ask for and collect it, and the capabilities and limitations of our existing and planned intelligence systems.

The US intelligence community is not solely to blame for its inability to adequately inform the policy maker. Rather, several external factors sustain its deep deficiencies. First, 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 and House committees on intelligence. Second, the majority of the budget for intelligence operations is managed by the Secretary of Defense rather than the Director of Central Intelligence. However, it is such a small proportion of the total Department of Defense budget that it merits very little oversight from the Secretary of Defense. Third, 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 policy makers are permitted to avoid investing in their own analysts. Furthermore, no one in Washington is held accountable for ignoring intelligence, and in fact most intelligence is disseminated in a fashion which makes it not only easy to ignore, but essential to do so. It is presented as a cumbersome compendium of classified research, often so compartmented that executive assistants are not cleared to read it, and so difficult to gain access to (codewords, signatures, special vaults) that the policy makers don't bother to seek it out.

The needs of the policy maker and the wont of the intelligence analysts are world apart. Four key contrasts between the two worlds are apparent.22 First, the analyst focuses on international data while the policy maker focuses on domestic political issues as the primary criteria for decision making. Second, the analyst is driven by community managers to produce *perfect* products over a lengthier time frame, while policy makers only requires *good enough* products immediately. Analysts continually run the risk of having no influence because their review process delays their product to the point that is overtaken by events. Third, the analyst is accustomed to integrating allsource information at the codeword level, while most policy maker staffs - and especially those implementing operational decisions - have at best a secret clearance. Therefore, a secret paragraph is better than a codeword page. Fourth, the analyst and community management focuses on substance and accuracy, while the policy maker 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. Lastly, the sources of unclassified (and unanalyzed) information available to the policy maker drown out and reduce to almost nothing the impact of the narrow inputs from classified intelligence. These competing influences on the policy maker, flooding him/her with verbal and written information,23 include: politicians (executive branch and legislative leadership, personal and professional staffs); government officials (department heads, assistant secretaries, program managers) and their message traffic; foreign officials and organizations; private and public sector (lobbyists, executives, citizen groups, pollsters, individuals); independent researchers (think tanks, academics, etc.); media and Internet; personal; and the intelligence community.

What does this mean? It means that at present the US intelligence community is unable to meet the most practical needs of the policy maker. At the same time the policy makers are unable to define and manage their own needs in the context of the funding available

for unclassified information procurement, and assert their prerogatives as intelligence consumers to dictate a new focus for national intelligence - one which stresses responsiveness to policy makers and the exploitation of open sources of information. Neither the US intelligence community, nor the information management specialists serving the policy makers, nor the policy makers themselves, have focused on the basic fact that intelligence is an inherent responsibility of command. It is the policy maker 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 3: PERILS AND PROMISE OF INFORMATION TECHNOLOGY

Up to this point, information technology (IT) has been a resource drain and ultimately has reduced the ability of government to hire and retain world class experts. It has imposed financial, productivity, secrecy, and opportunity costs on the policy maker. The "fire walls" between classified, policy maker, and private sector IT systems have created a wasteful and counter-productive archipelago of information, which the policy maker 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. IT offers extraordinary promise, but only if the policy maker begins to *manage* the technology rather than abdicate IT procurement decisions to technologists far removed from the core competencies of the policy environment.

In relation to content, IT appears to have swamped users with three waves, each of which has left them less productive and less informed than they were before having IT imposed on them. The "first wave," when electronic publishing and electronic storage of data first became possible, brought with it two major problems. First, because computer memory was so limited, the 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." Second, 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 problems. First, because the programs were so sophisticated, users were required to either spend a significant amount of time in training, or to forego most of the features offered by programs. Second, because the programs kept changing and managers kept allowing the technologists to specify ever-more sophisticated programs for use, the 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.

In the "third wave," the Internet has been 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 policy maker. However, it too imposes problems. First,

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. Second, 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; too many otherwise thoughtful professionals are accepting the Internet as the first and *last* stop in their quest for information. Furthermore, as one reflects on the approximately $300 billion dollars that the US intelligence community has spent primarily on IT and the roughly $3 trillion that the rest of the US Government has spent on IT (including for weapons and mobility systems) four costs emerge which must be considered by policy makers as they plan future IT investments.

Financial Costs

The ugly fact of the 1980s and 1990s is that IT usually provided a negative return on investment in both government and corporate applications, largely because of the dramatic impact on employee productivity and because of the lack of standardization across organizational lines. This interfered with data sharing and also wasted resources through the development of multiple variations of complex systems responding to different managers with the same functional requirements.24

Productivity Costs

The productivity costs of badly managed IT 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.25

Secrecy Costs

By classifying its vulnerabilities and its data, the US actually has become more vulnerable to electronic attack on its financial, communications, power and transportation infrastructures in the private sector. At the same time it has deprived most users of critical information.26 There is also "virtual secrecy," a pervasive compartmentation and concealment of information from the public and from the policy makers, which results from poor information management practices as well as bureaucratic regulations that block access to unclassified information.

Opportunity Costs

The US has spent billions on technical collection and related security systems and policies, which ensured the technical isolation of analysts dealing predominately with unclassified information. The result is a dysfunctional technological architecture. We have created barriers between different governments; between sectors (government, business, media, academy); between institutions within sectors; and between individuals within sectors who cannot readily share word processing or graphic files. This dysfunctional technological architecture is preventing policy makers 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 conflicts once begun.

In summary, today IT is part of the problem, not part of the solution. However, the fault does not lie with the technologist, but rather with the managers who have abdicated their responsibility for the direction of technology and its proper applications in support of core competencies.27 At the strategic level, we must manage information as the core value - what Paul Strassmann calls "knowledge capital" - and use IT to reach across national, organizational and disciplinary boundaries.28 At the operational level, the US must radically alter how it manages both security and procurement. Both currently are hobbling IT by placing barriers in the way of connectivity and state of the art capabilities, while simultaneously avoiding investment in advanced electronic security programming. At the tactical level, the US must dramatically realign funding from the collection of classified information, to the discovery, discrimination, distillation and dissemination of unclassified information. Finally, at the technical level, US intelligence must accept that its classified base of analyst workstations is a given and stop trying to create a duplicate architecture of unclassified machines which the analysts and policy makers will never use. Instead, it must rely on private sector "Sensitive Compartmented Information Facilities" to serve as the conduits for introducing unclassified information into the classified system. At the same time, we must invest in the global embassies (of all nations) and their related corporate offices and establish a "Global Information Management" concept of operations.

The field of imagery and global geospatial data illustrates the perils of badly managed information technology. US intelligence spent billions to collect repetitive snap-shots of (then Soviet) missile silo doors at the same time that the mapping satellite constellation was canceled 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 out-paced national assets in terms of diversity of utility and breadth of availability. For example, SPOT Image Corporation has most of the earth already in its archives, generally 100 percent cloud- free and less than three years old. Yet, the US 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.29 The Office of the Assistant Secretary of Defense has refused an even more modest request from NIMA for $25 million a year. The appropriate authorities continue to refuse to create a separate funding line for the procurement of commercial imagery. 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 government concerned with peace and prosperity. In 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. Thus, it is the foundation for virtual intelligence, virtual diplomacy, and information peacekeeping.

Now, what of the promise of information technology? Three areas merit attention: generic functional requirements for individual workstations; generic organizational methods for routine, reliable and responsive access to global data and expertise; and collaborative information-sharing across boundaries (See Figure 6).

The single most helpful contribution to the productivity of all those supporting leaders 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 stop 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.30 The essay has provided a few illustrative examples of generic requirements which should be part of joint government-corporate efforts to establish an international information technology standard that contributes to individual productivity.31 The technologists will be quick to say "we can do that," but there are two realities that continue to escape them. First, 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. Second, problems occur when multi-media and multi-lingual data can be obtained only from multiple remote sources. No technology should be considered acceptable until it has been fully tested against the real world data sources and data processing needs of the user. It is essential therefore, that policy makers 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, commander, and policy maker: the electronic information machine.

With respect to external access and the creation of an architecture through which leaders 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 of the prototype (Figure 7).32

Daily Intelligence Briefs

The lowest level of service is the *Daily Intelligence Brief*. It builds on a quality process that integrates multi-lingual access to the Internet, commercial media, and trade and industry journals as well as conference reports, dissertations, and new books in order to provide to each individual policy maker (or staff member) a concise digest of highly focused current news; each entry comes with a route to obtaining the full text document.

Help Desk

The next level of service, the Help Desk, provides rapid response online search and retrieval services that can access: the Internet; all major commercial online services (including international and foreign language service); international electronic databases

that are not necessarily online but can be exploited remotely; and hard-copy references, including general literature available in a major library.33

Experts On Demand

Even more expertise can be applied to a policy maker's problem by systematically identifying and then contracting with an individual expert who can bring to bear experience and immediate access to all manner of electronic and hard copy sources (as well as their own networks of experts and assistants). The economic benefits of out-sourcing decision support to such experts cannot be understated; this essentially allows the leader to harness expertise that has been maintained at someone else's expense and that has been validated in the academic marketplace through peer review 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

Finally, 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 to quickly identify and select from world-class experts on any topic. 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 source, 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 improve significantly 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 (See Figure 8).

The above cell is scalable, but the key idea is to avoid the creation of a centralized unit with increasing numbers of employees that attempts to actually do the research and develop the intelligence itself. Instead, focus for each of the specialists must be on "knowing who knows."34 The Internet specialist keeps track of external Internet experts who are also subject-matter experts (regional, scientific, or military) 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 focus on retaining the appropriate information broker or brokers. Each of these must have 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 with other directories, and direct calling. Their task is to rapidly get

answers to questions which 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 resources. Finally, the external specialist is a master of the marketplace and follows all of the niche providers who offer narrowly focused sources, software or services. Below are some of the standard niche services that are common to the private sector (See Figure 9).

Market research and studies and 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 constantly 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, etc.

Information technology continues to offer the policy maker significant opportunities for acquiring and managing knowledge with which to avoid 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 policy maker recognizes that in the age of information, management of information is an inherent function of command and not something that can be delegated to technologists. It is also critical that the policy maker focus on content and access to external expertise and multilingual 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. The cost of communication 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 (IT has an important but not an exclusive role to play in delivering this) will come from:

Discovery

Leaders 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 policy makers needs for discovering as much of the raw information as is necessary to meet the policy makers needs for "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. This is a labor-intensive process requiring genuine human expertise as well as new developments in automated understanding. A cost element also can be provided here, by giving the customer the benefits of superior knowledge in selecting sources of equal content but lower prices.

There are a number of major media providers, which can be accessed through the Internet for free, or through commercial online services for a fee.

Distillation

The essence of "intelligence," is 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.

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, video, electronic mail, etc.) is received by the intended policy maker , absorbed and is compelling enough to support action. There is far more to dissemination than simple delivery.35

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 leader and the intelligence community use open sources to the fullest extent possible, but then task the classified systems for such information as is truly critical. Moreover, they can utilize open sources to protect classified findings but also to inform those who require information support but to whom classified information cannot be disclosed.

PART 4: STRATEGIC INFORMATION MANAGEMENT

The private sector offers the policy maker an extraordinary range of world-class expertise at a very low cost and 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 policy maker. At the same time, he/she can acquire a new appreciation for information as a "munition" or a means by which to alter the balance of power in a conflict by altering the balance of information. In this section a new theory of "information peacekeeping" is presented. Its elements are (unclassified) intelligence, information technology, and electronic home defense. This article concludes that the private sector can be harnessed by the leader in a non-intrusive way, but that a national information strategy is required if the leader 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.

This final part of the article examines three elements which, taken together, can help avoid and resolve conflicts while significantly increasingly the productivity and

effectiveness of those practicing "virtual diplomacy": Information Archipelago; Information Peacekeeping; and Information Strategy.

Information Archipelago

The following figure illustrates the "information archipelago" essentially distributed private sector expertise and knowledge which exist today, the vast majority of it in the private sector.

Figure 10

In contemplating this archipelago,36 the policy maker should consider the following key findings. First, expertise contained within each of the sectors is created and maintained as someone else's expense. It 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. Second, the cost of this expertise, when the policy maker 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. Third, such published information as is available to the policy maker through either online retrieval or hard copy document retrieval represents less than 20 percent and more often less than 10 percent of what is actually known by the individual experts. Finally, the most significant deficiency in national intelligence today as it pertains to providing the policy maker with just enough, just in time "intelligence," is lack of direct access to the expertise available in the private sector. There are many examples of worthy private sector sources and capabilities that 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.

At 1700 hrs on 3 August 1995, after testifying to the Commission on Intelligence regarding the importance of dramatically improving government access to open sources, the author was invited to execute a benchmark exercise in which he and the US intelligence community simultaneously would seek to provide the Commission with information about the chosen target, Burundi.37 By 1000 on 7 August 1995, the author had delivered the following 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; and 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 citation 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, I acquired a list of the top journalists in the world whose by-line reporting on Burundi suggested their familiarity with the situation. The Institute of Scientific Information provided me with a list of the top academics in the world publishing on the Burundi situation, together with contact information. East View Publications provided a list of all immediately available "Soviet" military topographic maps of Burundi, at the 1:100,00 level. SPOT Image Corporation determined that it could

provide digital imagery for 100 percent 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 nap of the earth interactive aviation and ground mission rehearsal simulation packages.38

The above effort has received wide recognition among those responsible for oversight of the US intelligence community. One very senior hill staff manager described at as "John Henry against the steel hammer - only John Henry won." The "steel hammer," the US intelligence community, had nothing of substance, because Burundi was the very bottom of its priority list and capabilities were not suited for surge coverage of this obscure and remote area that previously had been irrelevant to US interests. However, it is very important to stress again that open sources are not a substitute for spies and satellites. Rather, both common sense and fiscal realities suggest that is imperative that the policy maker be able to exploit open sources to the fullest in their public diplomacy, military acquisition and economic competitiveness roles. They should rely on classified intelligence presented in the context of open sources for those unique insights and detail which cannot be obtained through other means and which in fact are demonstrably so precious as to warrant the risk and cost of espionage.39

Information Peacekeeping

Information Peacekeeping is the active exploitation of information and IT in order to modify the balance 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); IT (providing tools which allow the recipient to access international information and the ability to communicate with others); and electronic home defense, a strictly defensive aspect of information warfare.40 Information Peacekeeping is *not*: the application of IT in support of conventional military peacekeeping or humanitarian assistance operations; the development and execution of traditional psychological operations which focus on manipulating perceptions and imposing strategic deceptions; or covert media agents of influence or paramilitary operations. Nor is it clandestine human intelligence. However, there are some "gray areas." For example information peacekeeping may require the clandestine delivery of classified or open source intelligence, or the covert delivery of tools (cellular phones, fax machines, personal computers and software); or it 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 likely to be most powerful and most effective when it relies exclusively on open sources of intelligence and on overt action and, therefore, when it is 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, are as follows. First, policy options have to start "here" at home, and now during violent "peace." Second, information peacekeeping is the

ultimate global presence. Third it, is the first policy option - both to ensure that the policy maker has a full knowledge of the situation and to impact constructively on those we seek to influence. Moreover, there is a 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 elements of national intelligence into a larger global information architecture. Information is the ultimate *countervailing force* against emerging threats and the most cost-effective means of devising diplomatic and other responses intended to avoid or resolve conflicts.41

At least 80 percent of the information the policy maker needs to conduct information peacekeeping operations is not controlled by the government and is only available from the private sector. "Knowing who knows" and the creation of management, technical, security and procurement architecture which permit harnessing distributed intelligence, is the emerging new source of national power. However, because the policy maker is inundated with contradictory information lacking methodical evaluation, a vital 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 *cannot* succeed without a mastery of open sources of information. In fact, multi-channel delivery of "truth" is the SIOP42 of the information age.

Information peacekeeping is an information-intensive process with both mass and niche audiences. It 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 leader will be to manage a national intelligence architecture which can identify rapidly the information center of gravity, prepare the information "battlefield," and deliver the appropriate (non-lethal) information "munitions" to carry the day.

Figure 11

Information peacekeeping starts and succeeds with intelligence - accurate and comprehensive analyzed information tailored to the needs of the policy maker and useful to the participants in the emerging or on-going conflict. While always the fundamental aspect of information peacekeeping, intelligence must be developed in full consonance with both an IT 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 object 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 national information architecture fully integrated into a global information architecture of knowledge.43

Information Strategy

There are four elements to a national information strategy that can empower those who would seek to practice virtual diplomacy and avoid or resolve conflicts:

Connectivity. To prevent any confusion about connectivity being "virtual" strategy, it is useful paraphrase the observation of the former Commandant of the Marine Corps: "Connectivity without content is *noise;* content without connectivity is *irrelevant.*"44 The National Information Infrastructure (NII) and Global Information Infrastructure (GII) are brillant initiatives, but they are seriously flawed in that they do not address issues of content. Nor do they explain how the policy maker can use the NII and GII to nuture distributed centers of expertise and fully integrate, in real time, the classified intelligence available from selected elements of the government, unclassifed government information, and the often more accurate, comprehensive and lower-cost information available from the private sector.

Content: The private sector will not subject itself to control or regulation by the intelligence community, nor will it cooperate with any initiative that 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 nurtures selected scientific and technical initiatives. A National Knowledge Foundation (NKF), funded with just $1 billion a year 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" burden-sharing agreement could reduce radically the cost of information for Third World and other policy makers and begin the process of creating an "information commons"45 that can support virtual diplomacy.

Coordination: There is an urgent need for voluntary coordination in the arenas of standard 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.

Communication And Computing Security: The vulnerabilities of our financial, communications, power and transportation infrastructure, all with very heavy computational aspects which are easily attacked by both physical and electronic means, are just now emerging into the public idea, despite a decade of effort by innovative thinkers such as Winn Schwartau.46 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 age.47

CONCLUSION

The day of the decision maker oblivious to intelligence is over. US leaders need to know about the world in terms and by means that impact on their 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 policy maker have adequate access to the wealth of information available in the private sector. In the face of ambiguous unconventional threats, if we do not reform our community, major intelligence failures are waiting to happen. Decision cycles are compressing in time and extending in scope. All intelligence systems must be geared to cold-starts, surges, and answering specific questions from specific decision makers. 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. It also can empower the policy maker by making possible the execution of a new form of global power, information peacekeeping. The key is to mobilize all knowledge sectors (experts and knowledge created and maintained at *someone else's expense*). "Knowledge about knowledge" is the core competency of the twenty-first century intelligence professional.

The real good news is that in comparison with the funding of military systems, contingency operations, disaster relief and many other 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 is easily affordable in the context of $3 billion per year in savings from improvements in the management of unclassified IT and $10 billion per year in savings from refocusing classified IT toward "the hard stuff."48 The US can become a "Smart Nation" able to practice information peacekeeping. But, 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 - it is a step toward the formulation of knowledge strategies needed either to fight or forestall the wars of tomorrow.49

Endnotes

The original version of this article was distributed at the Virtual Diplomacy Conference sponsored by the US Institute of Peace (Washnington, DC, 1-2 April 1997). It is available electronically at www.oss.net/VIRTUAL. This version will become available following publication at www.oss.net/Conres.

1. This is a generalization. The record of ULTRA during World War II clearly shows the value of and the need to protect certain kinds of intelligence. In the author's experience, there are very few signals and human intelligence operations whose extraordinary value is directly translatable into action through communication to a very small number of decision makers. But on the whole intelligence is vastly more valuable when security classification does not interfere with dissemination of the message to key consumers.

2. "If it is 85% accurate, on time, and I can share it, this is a lot more useful to me than a compendium of Top Secret Codeword materials that are too much, too late, and require a safe and three security officers to move around the battlefield." Paraphrase of comment by a Gulf War veteran Navy Wing Commander, made at Technology Initiatives Game 1992. See also Hugh Smith, "Intelligence and UN Peacekeeping," Survival, 36 no. 3. (Autumn 1994), p. 175, "the concept of UN Intelligence promises to turn traditional principles on their heads. Intelligence will have to be based in information that is collected primarily by overt means, that is by methods that do not threaten the target state or group and do not compromise the integrity or impartiality of the UN."

3. Paul Evan Peters, Executive Director of the Coalition, has related this fashionable phrase to global networks for networking information. Speaking to the International Document Acquisition conference in 1994, he noted that it makes sense to archive vast volumes of material centrally if one can reach out and get exactly what is needed on a "just in time" basis. To this the author would add two caveats first, that only 10 percent of what one needs is generally online, although online means can be used to reach experts who have access to the other 90 percent. Second, the most exciting aspect of distributed information is that someone else bears the cost of creating and updating such information as is available online, and for maintaining the expertise, both of which tend to be more current and insightful.

4. The most common objection to this idea, generally from intelligence analysts rather than the policy makers themselves, has been founded on an extreme reluctance to reveal their organizational interest or the nature of their question.

5. The most reliable source on world class subject experts is provided by the Institute of Scientific Information. It maintains an exclusive international, multi-lingual database of those who have not only published in peer-reviewed journals, but also been cited by their peers in a manner which easily establishes their general influence and credibility. These experts in turn generally know their peers in government and non-government institutes and organizations who are world-class authorities but cannot publish.

6. The EARTHMAP report, signed off in October 1995 by Under Secretary of State Tim Wirth and other principals, is an eighty-person multi-agency finding that specifies the critical nature of comprehensive global mapping in support of economic and environmental initiatives. Unfortunately, the US intelligence community and the Department of Defense have both chosen to ignore the EARTHMAP Report and declined to respond to the urgent civilian agency needs for maps in support of peacemaking and diplomacy. They are also ignoring increasingly insistent demands from the US theater

commanders-in-chief for wide-area surveillance that can be obtained from commercial imagery sources. In November 1998, the National Imagery and Mapping Agency (NIMA) declared in a press release that it was earmarking $ one billion over five years for the procurement of commercial imagery. This is nothing more than a continuance of the status quo and a callous disregard for increasingly troublesome shortfalls. The established requirement for commercial imagery was articulated in 1996 at $250 million per year at the 10 meter level of resolution, and in 1997 at $500 million per year at the one meter level. Hence, the current NIMA program addresses less than 10 percent of the requirement.

7. A complete copy of the model, including war-fighter definitions of high, medium, and low degrees of difficulty for each of 107 factors (43 military, 35 civil, and 29 geographic) is now available to US government personnel as Appendix F-1 in Open Source Intelligence: Professional Handbook 1.1 (Joint Military Intelligence Training Center, October 1996). A copy of the handbook (less chapter 6 and appendices F and G) is available at: http:www.oss.net>. The author's contribution to the model (developed by a team) was significantly influenced by Edward N. Luttwak, STRATEGY: The Logic of War and Peace (Cambridge, MA: Harvard University Press, 1987), in which he demonstrated the inter-relationship between weapons systems at different levels of war, each perhaps irrational in isolation, but most sensible when considered as part of the whole.

8. United States Marine Corps, Overview of Planning and Programming Factors for Expeditionary Operations in the Third World (Marine Corps Combat Development Command, March 1990) was an unique first effort for the US intelligence community as a whole. It developed strategic generalizations founded on a close working relationship with the "warfighter" customers, who specified the 69 countries to be considered; defined the military , civil, and geographic factors of greatest interest to them (as well as difficulty); and used open sources of information exclusively, publishing the results in unclassified form. It is available today as a recurring global coverage study, Expeditionary Factors (FOUO/RESTRICTED).
Return to Article

9. The 90 percent figure has not changed in the seven years since the study was done. In September 1996, official unclassified Defense Mapping Agency briefings confirmed that while most of the world is charted at the 1:1,000,000,000 level and much of it at the 1:250,000 level, only 10 percent of the world is available at the 1:50,000 level (10 meter resolution) where the hard work of coalition and fire support coordination takes place. This 10 percent is generally old data. For the specific Marine Corps study, we found that of our 69 countries of high interest, most in the Third World, we had no 1:50,000 maps at all for 22; old 1:50,000 maps for the ports and capital cities only for another 37, and very old 1:50,000 coverage for 10 countries.

10. We still do not have a proper Table of Organization and Equipment for a unit to handle refugees and prisoners of war. In the Gulf War, this became an undesirable duty for the nearest infantry battalions. In particular, such tables as exist for reserve units do

not provide for the communications and computing equipment, nor the special personnel, needed to rapidly debrief individuals and enter the findings into the larger information architecture.

11. The figure is slightly revised from an original developed by the author: Robert David Steele, "Internal War: A Framework for the Prediction of Revolutionary Potential," unpublished graduate thesis, Lehigh University, May 1976.

12. See General Alfred M. Gray [Commandant of the Marine Corps], "Global Intelligence Challenges in the 1990's," American Intelligence Journal, (Winter 1989-1990). The author has subsequently developed this theme with an illustrated chart in his article "The Transformation of War and the Future of the Corps," in INTELLIGENCE: Selected Readings Book One (Quantico, VA: Marine Corps Command and Staff College, 1992-1993), and in "Private Enterprise Intelligence: Its Potential Contribution to National Security," Intelligence and National Security, 10 no. 4, (October 1995) pp. 212-28.

13. John Peterson, president of the Arlington Institute, developed the original matrix to show how we are too focused on "war, over there" while failing to develop our capabilities for defending ourselves here at home, within a "violent" peace. The author has added the third dimension of time.

14. In his first few days as Secretary of Defense, William S. Cohen told the media that his greatest problem was coping with the enormous flow of information that floods his office and crowds out any time for reflection. "The unrelenting flow of information, the need to digest it on a minute-by-minute basis, is quite different from anything I've experienced before." Washington Post, 5 March 1997, p. A22. This is a management and staff failure.
Return to Article

15. Policy makers' memoirs buttress many of the conclusions reflected in this paper. See, for example, George Shultz, Turmoil and Triumph: My Years as Secretary of State (New York: Scribner's, 1993), pp. 50, 297, 307, 312, 425, 492-93, 544, 595, 619. These pages provide a litany of intelligence problems. See also, Colin Powell, My American Journey (New York: Random House, 1995), p. 293: "I preferred the Early Bird with its compendium of newspaper stories (to the President's Daily Brief)."
Return to Article

16. "In some areas, such as economic analysis, it is estimated that as much as 95% of the information utilized now comes from open sources . . . an adequate computer infrastructure to tie intelligence analysts into open source information does not appear to exist . . . [this] should be a top priority of the DCI, and a top priority for funding." Preparing for the 21st Century: An Appraisal of U.S. Intelligence. Report of the Commission on the Roles and Capabilities of the United States Intelligence Community (Washington, DC: 1 March 1996), pp. 88-89

17. See, Loch Johnson, "Seven Sins of Strategic Intelligence," World Affairs, no. 146 (Fall 1983), pp.176-204. This theme is repeated in the two major intelligence reviews

completed recently: Preparing for the 21st Century: An Appraisal of U.S. Intelligence (1996); and IC21: Intelligence Community in the 21st Century (Washington, DC: House Permanent Select Committee on Intelligence, 4 March 1996). The author gained an interesting insight into "why" this problem persists from reviewing correspondence between the (then) Deputy Director of Intelligence, Richard Kerr, and the (then) Chairman of the Senate Select Committee on Intelligence, Senator David Boren. Kerr declined the offer of large scale funding for another satellite system, but requested funds for the processing of the volumes of information already being collected; those funds were not provided. According to authoritative senior officers, the US processes less than 10 percent of the imagery and SIGNT it collects. Sadly, it is a bureaucratic reality that very large expensive technical collection systems with single focal points for management in the administration and for the authorization on the Hill, are far easier to work with than inter-agency cross-committee systems of lesser cost and much greater importance to improving government operations as a whole.
Return to Article

18. Among the better books on the topic of analysis are: David A. Charters, Stuart Farson, and Glenn P. Hastedt, eds., Intelligence Analysis and Assessment (London: Frank Cass, 1996); John A. Gentry, Lost Promise: How CIA Analysis Misserves the Nation (Latham, MD: University Press of America, 1993); and, Angelo Codevilla, Informing Statecraft: Intelligence for a New Century (New York: Free Press, 1992). Even the recently retired Deputy Director of Intelligence at CIA, Douglas McEachin, has been quoted that "it is impossible to do good strategic analysis with a bunch of 19 year-olds on two year rotations." "Hiring to payroll" and the deliberate focus on technical collection rather than human analysis has left both the national and defense intelligence communities with insufficient funds to hire world-class analysts across the board, and with almost no funds with which to consult world experts in the private sector.

19. This table is adapted and updated from the Robert D. Steele, "A Critical Evaluation of U.S., National Intelligence Capabilities," International Journal of Intelligence and Counterintelligence, 6, no. 2 (Summer 1993) pp. 175-83 where extensive commentary is provided on each of the above deficiencies.

20. "Improving National Intelligence Support to Marine Corps Expeditionary Forces: General Areas of Interest," a published unclassified paper staffed by the author in the aftermath of the Gulf War as part of Marine Corps contribution to the defense intelligence restructuring effort in the early 1990s.

21. When the author was a member of the Foreign Intelligence Requirements and Capabilities steering group for the US intelligence community in the early 1990s, there was a brief discussion of shifting from "priority driven" to "gap driven" collection, to ensure that once key collection was accomplished against higher priority targets that basic collection was undertaken against lower priority targets. The group chose to continue business as usual, with the result that Russian border guard transmissions take precedence over Chinese dissidents or Indian nuclear testing signals. A "gap driven' collection strategy would be an ideal means of integrating the capabilities of the overt

"virtual intelligence community" with those of classified community, and would make a possible a coherent strategy by which overt sources provide global coverage as well as contextual support for narrowly targeted classified collection.

22. From the presentation by Summer Benson, former CIA analyst, to CIA's 1986 senior class on "Intelligence Successes and Failures" (now discontinued). See also, two other detailed tables (contrasting the needs of policy makers and the wont of analysts) taken from the 1992 Harvard Executive Program (Intelligence Policy), in Steele, "A Critical Evaluation" IJIC (1993), p. 187.

23. This material is also drawn from the CIA course on "Intelligence Successes and Failures."

24. The author wishes to acknowledge the contribution of Paul Strassmann, former Director of Defense Information and the former Chief Information Officer of the Xerox Corporation in understanding this issue. Strassmann identified a potential savings of $22 billion over seven years through straightforward improvements in US government information technology "housekeeping." In addition, his in-depth study of Fortune 500 investments in information technology has shown that these are randomly associated with productivity and the generation of "knowledge capital"™ (Mr. Strassmann's term).

25. Captain Patrick Tyrell, RN then on detached assignment from his position as deputy to the Assistant Chief of Staff for C3I, remarked at an Information Warfare Conference in Brussels in May 1996, that managers must "take back control" from technologists and refocus information technology investments on the functional needs of their key personnel.

26. See the report of the Commission on Protecting and Reducing Government Secrecy, (Washington, DC: US Government Printing Office, 4 March 1997).

27. In 1991, Admiral Jerry Tuttle, USN, the "Rickover" of the information age, sponsored Technology Initiatives Game 1991 at the Naval War College. The two most dramatic conclusions reported to the Chief of Naval Operations were: first, technology is not the showstopper; management is where we must change the way we do business. Second, we must define a completely new paradigm of what information we need, how we handle it, and how it is delivered to the user. This new paradigm must include an information architecture (vice a system/command architecture) approach, must extend to include commercial and coalition capabilities, and must integrate Geographic Position System data.

28. These four points comprise the essence of the author's invited presentation to the Advanced Information Processing and Analysis Steering Group of the US intelligence community conference in 1996.

29. NIMA today spends around $20 million/year to purchase SPOT (10 meter) and other (Russian 2 meter, Indian 5 meter, Canadian 25 meter) image data. Despite a clear

awareness within NIMA of the urgent need to spend heavily for wide-area surveillance coverage from commercial imagery, severe bureaucratic resistance continues.

30. While serving as a founding member of the Advanced Information Processing and Analysis Steering Group of the Intelligence Research and Development Council, the author observed that virtually every "black" compartmented program appeared to be allocating around $10 million a year to building its own "all source fusion workstation." Since the data domains were compartmented, the procurement system was essentially funding between 10 to 20 different versions of the same generic workstation. The author's second graduate thesis, "Strategic and Tactical Information Management for National Security," (unpublished thesis, University of Oklahoma, May 1987) influenced his perceptions on the vertical and horizontal disconnects that permeate the entire US government information infrastructure.

31. The requirements were developed by the author in 1996 while serving as Project Manager for "Project GEORGE (Smiley)" on the Artificial Intelligence staff, Office of Information Technology, CIA. A similar requirements document, "Computer Aided Tools for the Analysis of Scientific & Technology (CATALYST)" was developed by the Office of Scientific and Weapons Research under Dr. Gordon Oehler. The Office of Information Resources promptly informed them that their requirements, which required Sun and other UNIX workstations, could not be accommodated because CIA had decided to go with IBM and the PC2 architecture.

32. This model for service delivery has been developed by Jan Herring, a founding member of the Society of Competitive Intelligence Professionals (SCIP), and a widely recognized as one of the founding fathers of the profession of "business intelligence." After a full career as an analyst, in the US intelligence community, retiring in 1983 as the National Intelligence Officer for Science & Technology, he was invited by Motorola to establish the first major business intelligence unit in the United States, and went on to do the same for several other major corporations.

33. In the early 1990's the CIA created a list of all public journals to which its analysts had access through their library, by subscription, or via electronic means. They found that roughly 20 percent were available through LEXIS-NEXIS, 20 percent through DIALOG, and 20 percent through other online services or other electronic databases; 40 percent were not online. Most information brokers rely largely on either LEXIS-NEXIS or DIALOG, not both in tandem, and have limited access to the larger range of international online sources, while having almost no access at all to a complete collection of hard-copy references. Very few information services customers understand that the best value in searching comes from employing a searcher who has both access to a full range of international sources, and subject matter expertise; otherwise, the customer pays for the searcher's learning curve and false trails. The Burwell World Directory of Information Brokers is an essential reference for this. It provides both a subject-matter index to information brokers, and an index to brokers speaking a foreign language and familiar with specific foreign databases.

34. The author credits this excellent phrase to Dr. Stevan Dedijer, a veteran of the OSS and former professor at the University of Lund, Sweden, considered by many in Europe and elsewhere to be intellectual father of the concept of business intelligence.

35. Then National Security Advisor Frank Carlucci told a group of mid-level CIA analysts in the 1980s that the ideal intelligence briefing for President Ronald Reagan would be "a five minute video, five minutes before his meeting." This remains a superb statement of the requirement, and one that the intelligence community has yet to acknowledge or address.

36. The author first developed an open source exploitation strategy in 1989 when he discovered the data vacuum within the classified world while standing up the Marine Corps Intelligence Center. After first running several international symposia that brought together leading experts, the author published two formal papers in this area. The first (written under contract to a representative of a European government), "ACCESS: Theory and Practice of Intelligence in the Age of Information" (26 October 1993), was the first comprehensive attempt to examine why national governments must radically alter their investment strategies to better integrate unclassified government information with private sector information, reserving the classified investment for "the hard stuff." The second, "ACCESS: The Theory and Practice of Competitor Intelligence," was developed as a keynote presentation to the Association for Global Strategic Information, meeting in Heidelberg, and was subsequently published in the Journal of AGSI (July 1994).

37. See Preparing for the 21st Century: An Appraisal of U.S. Intelligence (1996), p. 88. What the report does not mention is that the comparison was so shockingly graphic that the staff initially decided to avoid the issue of open sources entirely, calling the exercise "unstructured and invalid." This "denial" was common knowledge within 48 hours, and subsequent correspondence with the Chairman evidently was successful; a three person sub-panel of members was created, and the report ultimately contained a number of very significant comments on the critical importance of improving access to open sources of information. Perhaps even more significant was the Commission's conclusion that intelligence questions which could be answered mostly from open sources should be answered by the consumers themselves by the organizations of the leaders needing the intelligence. This is an important recommendation which validates much of this article's thrust, because policy makers can no longer excuse their ignorance by claiming reliance on secrets that do not materialize. They must take responsibility for collecting and producing open source information. However, most of them do not have the staffs or funds to perform the tasks necessary to convert open source information into open source intelligence.

38. SPOT Image Corporation was not part of the author's consortium of open source providers during the exercise, but was identified later and its offerings with respect to Burundi reported. Subsequently, it will take the US commercial imagery providers at least a decade to replicate the powerful system that SPOT has in place today, including

multiple satellites with two day revisitation capabilities, seventeen ground stations, and virtually the entire world available in the archives for immediate exploitation.

39. Authoritative sources suggest that about 80-90 percent of US government secrecy is derived from a desire to protect bureaucratic interests rather than true national security. On this see Rodney B. Mc Daniel, (then) Executive secretary, National Security Council and former Senior Director (White House) Crisis Management Center, quoted in Thomas P. Coakley, ed., C31: Issues of Command and Control (Washington, DC: National Defense University Press, 1991), p. 68.

40. The author developed the concept of information peacekeeping in 1994 in a discussion with James Roberts, the Director of Intelligence and DOD principal action officer for psychological operations in the Office of the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict.

41. See Alvin Toffler, Powershift: Knowledge, Wealth, and Violence at the Edge of the 21st Century (Batham 1990); and Alvin and Heidi Toffler, War and Anti-War: Survival at the Dawn of the 21st Century (Boston, MA: Little Brown, 1993).

42. Strategic Integrated Operations Plan, a term originally applied to warplans for use of strategic nuclear forces.

43. See Robert D. Steele "Creating a Smart Nation: Strategy, Virtual Intelligence and Information Warfare," in Alan D. Campen, Douglas H. Dearth, and R. Thomas Gooded, contributing eds, CYBERWAR: Security, Strategy, and Conflict in the Information Age (Washington, DC: AFCEA, 1996); and "Creating a Smart Nation: Strategy, Policy, Intelligence, and Information," in Government Information Quarterly, (Summer 1996). See also: "Smart Nations: National Information Strategies and Virtual Intelligence Communities," Defense Review (April 1996); and "Reinventing Intelligence: The Vision and the Strategy," International Defense Review (December 1995).

44. General Alfred M. Gray, testifying to Congress in the 1990s, actually said, "Communications without intelligence is noise; intelligence without communication is irrelevant."

45. The concept of the "information commons" was originated by Lee Felsenstein of the Interval Research Corporation.

46. Winn Schwartau's 1994 book INFORMATION WARFARE: Chaos on the Electronic Superhighway has become the classic work, and done more than any other single work to heighten international awareness of our general vulnerability to electronic attack.

47. A major government organization intercepted each piece of hardware and software reaching its loading dock over a one-year period, and subjected every item to intensive testing. It found 500 distinct computer hardware and software viruses during this period, in items coming shrink-wrapped directly from the factory. A major reason that it is not

safe to work and play in cyberspace is that no one has defined "due diligence," and the industry therefore, is not criminally liable. Nor are managers of intellectual property being held liable by stockholders for failing to protect that property from electronic theft.

48. In 1994, then DCI James Woolsey agreed in an interview that the US intelligence community could safely plan to reduce its annual budget from $30 billion a year to $20 billion a year. This was announced publicly by Dr. Loch Johnson, then a staff member on the Commission on Intelligence, during his keynote speech to the Fourth International Symposium on "Global Security and Global Competitiveness; Open Source Solutions," 1994. See also Robert D. Steele, "Intelligence and Counterintelligence: A Proposed Program for the 21st Century," White Paper, (14 April 1997) at www.oss.net/OSS21, $11.6 billion a year in cuts, are itemized, together with $1.6 billion a year in off-setting increases. While the author would prefer not to cut the US Intelligence budget, but rather realign funds within the community, the DCI's lack of programmatic authority requires that the "out of control" investment by the National Reconnaissance Office, the National Security Agency, and the NIMA be called into question.

49. Toffler, War And Anti-War, p. 164.