INFORMATION PEACEKEEPING: THE PUREST FORM OF WAR*

Robert D. Steele

Information Peacekeeping is one of two neglected aspects of Information Operations, a new concept that up to this point has focused almost exclusively on Information Warfare, and avoided dealing with the substance of All-Source Intelligence, or the proactive possibilities of Information Peacekeeping. Information Peacekeeping is the active exploitation of information and information technology so as to achieve national policy objectives. The three elements of Information Peacekeeping, in order of priority, are open source intelligence; information technology; and electronic security and counterintelligence. Information Peacekeeping is the strategic deterrent as well as the tactical force of first resort for the 21st century. Virtual Intelligence, a supporting concept, is the foundation for informed policy-making, judicious acquisition management, effective contingency planning and execution, and timely public consensus-building. By its nature, Information Peacekeeping must rely almost exclusively on open sources and services available from the private sector; this requires the crafting of a new doctrine of national intelligence that places the critical classified contributions of the traditional national intelligence communities within the context of a larger global information community. Information Peacekeeping is the purest form of war, but most traditional warriors will be reluctant to accept its most fundamental premise: that intelligence is indeed a virtual substitute for violence, for capital, for labor, for time, and for space. Information Peacekeeping is in effect both a strategy for government operations and a national security strategy with global

* In Alan Campen and Douglas Dearth, *CYBERWAR 2.0: Myths, Mysteries, and Realities*, AFCEA Press, June 1998, pp. 277-293.

“Information Peacekeeping: The Purest Form of War”, in Lloyd J. Matthews (ed.), *Challenging the United States Symmetrically and Asymmetrically: Can America be Defeated?* (Strategic Studies Institute, U.S. Army War College, July 1998), pp. 143-171.

reach; consequently it has profound implications for how we train, equip, and organize our government and our military.

Introduction: Intelligence as Munition.

Time and time again, the U.S. defense and intelligence communities rush to spend billions on technology, while routinely ignoring the challenges and opportunities inherent in human collection, open-source collection, foreign area expertise, and human all-source analysis.[1] We do it in mobility systems, in weapons systems, in command-and-control systems and in intelligence systems. Sadly, leaders in all corners of the Department of Defense (DoD), at all levels, continue to abdicate their responsibility for *thinking* at the strategic, operational, tactical and technical levels, and have surrendered their forces to the mindless flow of self-generated bits and bytes.[2]

A majority of the U.S. military leadership still does not "get it." The Revolution in Military Affairs is a joke. It is nothing more than lip service, substituting astronomically expensive systems with no sensor-to-shooter guidance nor any relevance to three of the four warrior classes, for outrageously expensive systems with no sensor-to-shooter guidance and dated relevance to one of the four warrior classes. The three warrior classes we must confront in this new era are: the low-tech brutes (transnational criminals, narco-traffickers, terrorists); the low-tech seers (ideological, religious, and ethnic groups unable to accept conventional relations among nations); and high-tech seers (a combination of information terrorists or vandals, and practitioners of economic espionage).[3] Most of our training, equipment, and operational doctrine are completely unsuited to meeting the threat from these three warrior classes. Perhaps even more disturbing is the fact that our national "order of battle" must now fully integrate our government civilian agencies and our private sector information reserves, but we have no one in a leadership position who is willing or able to deal with this harsh and urgent reality.

The real revolution is being led by a few original thinkers who have yet to be heard on Capitol Hill and whose thoughts are a decade from effecting fruitful changes in how we train, equip, and organize our nation for war. Alvin and Heidi Toffler were among the first to articulate the fact that information is a substitute for wealth and violence, for capital, labor, time, and space.[4] Pilots and ship drivers may never forgive Martin Libicki for reframing their platforms as delivery vehicles for intelligence-driven operations.[5] Winn Schwartau overcame his Hollywood and rock-and-roll past ultimately to inspire a Presidential Commission on Critical Infrastructure Protection.[6] Colonel James Clark blew past the naysayers, with support from the Vice Chief of Staff of the Air Force to bring EAGLE VISION in as an operationally effective means of putting real-time commercial imagery into tactical service—something the National Reconnaissance Office (NRO) and the National Imagery and Mapping Agency (NIMA) refused to contemplate and still resist at every level.[7]

Information Peacekeeping,[8] the subject of this paper, is the purest form of war. It shapes the battlefield, it shapes the belligerents, and it shapes the bystanders in such a way as to defeat the enemy without battle—in such a way as to achieve U.S. policy objectives without confrontation and without bloodshed. Sun Tzu would approve.[9]

At the strategic level Information Operations (Figure 7) must be seen as a triangle in which all-source intelligence, information warfare, and information peacekeeping are seamlessly integrated and inherent in all aspects of military and civilian operations. *Perhaps the most important aspect of information operations in the 21st century is that it is not inherently military; instead, civilian practitioners must acquire a military understanding and military discipline in the practice of information operations, if they are to be effective.*

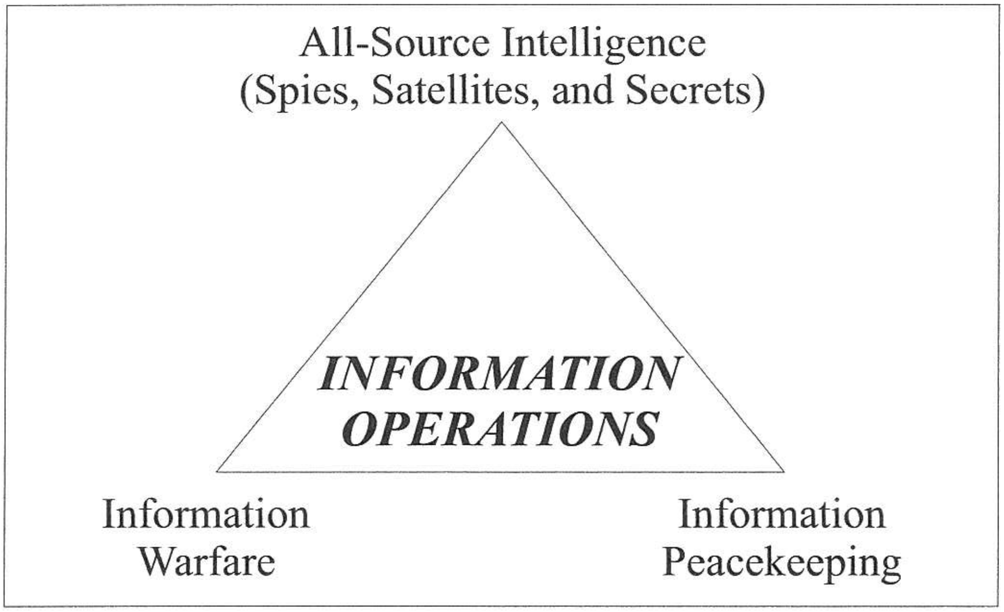

Figure 7. Strategic View of Information Operations.

Information Operations tend to be viewed as a strategic form of Information Warfare, but this is a much too narrow view which deprives the policymaker, acquisition manager, and commander of two-thirds of the "firepower" represented by a more accurate and well-rounded understanding of Information Operations.

All-Source Intelligence is the critical classified element of Information Operations which assures all parties being supported that they are receiving essential indications and warning intelligence, current intelligence, and estimative intelligence, to name just a few kinds of all-source intelligence.

Information Peacekeeping is the active exploitation of information and information technology so as to achieve national policy objectives. The three elements of Information Peacekeeping, in order of priority, are: open-source intelligence; information technology; and electronic security and counterintelligence.

Information Peacekeeping is a *strategic deterrent* that radically increases the ability of the practicing nation to avoid or resolve conflict in relation to all four warrior classes and across the complete spectrum of government operations—not only military but diplomatic, commercial, agricultural, etc.

All three aspects of Information Operations—the obvious one of Information Warfare and the two less obvious aspects of All-Source Intelligence and Information Peacekeeping—share one critical component: open-source intelligence (Figure 8). No aspect of Information Operations can be conducted effectively without full access to a cooperative private sector that controls the vast majority of national knowledge resources—the "information commons."[10] Once thought of in this light, it becomes evident that the center-of-gravity for Information Operations is in the civil sector—the private sector.

Interestingly, this perspective also makes it clear that the importance as well as the presence of secrecy declines dramatically as one moves from the left "warfare" side of the equation to the right "peacekeeping" side of the equation. In fact, fully 80 percent of the intelligence "solution" comes

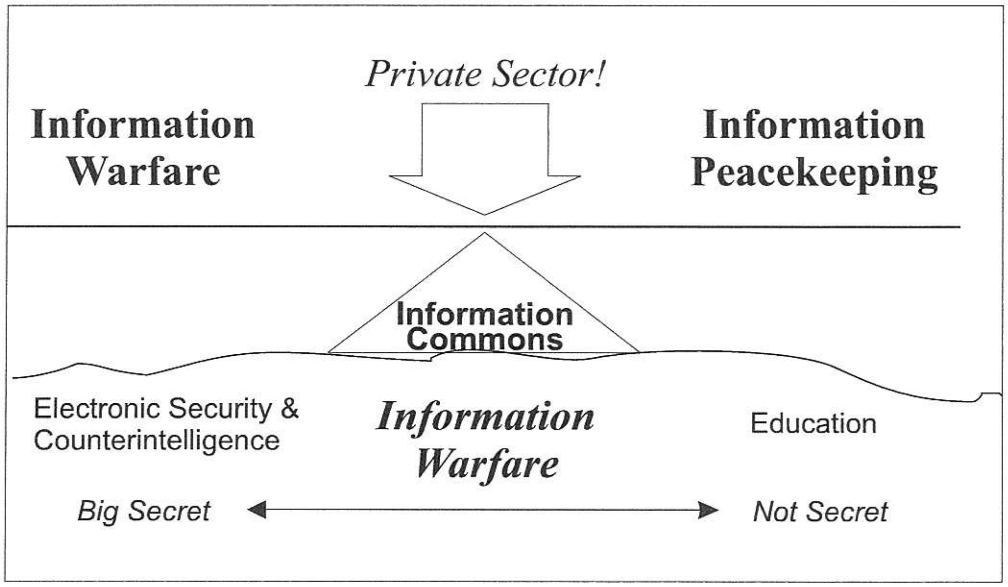

Figure 8. The Center of Gravity for Information Operations.

from open rather than classified sources, and it is incumbent on the consumers of intelligence—not the producers—to harness these *open* sources.[11]

Consumer Communities: Getting Back to Basics.

For those tempted to question the substantial depreciation in the value of secrecy, a glimpse into the cognitive battlefield—the mind of a typical consumer—is instructive (Figure 9). The four consumer communities—the policymakers, the acquisition managers; the commanders and their staffs; and the public—each require tailored intelligence which is largely unclassified in nature, collected and delivered in very short time-cycles, and often most valued when it is least cumbersome (i.e., concise and to the point). The public must be treated as a real-time partner to decision making in foreign and defense policy. The policymaker needs, and must use, tailored open-source intelligence products to ensure that the public is informed

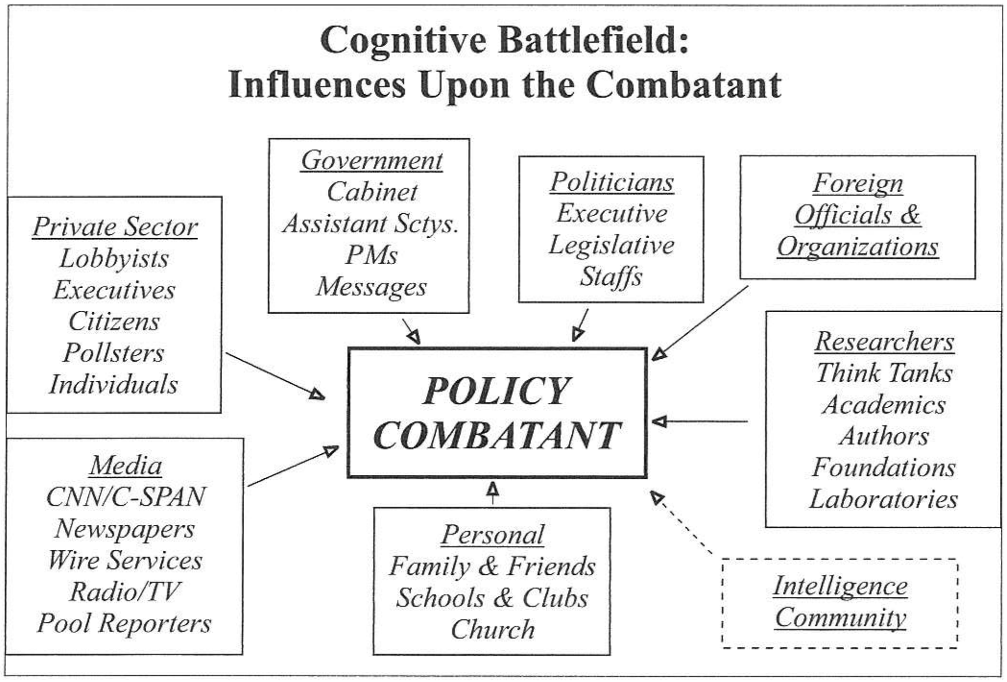

Figure 9. Understanding the Cognitive Battlefield.[12]

enough about a situation to support administration decisions both during and after the fact.

This boils down to two major facts in the world of Information Operations:

1. Ninety percent of the information reaching a typical consumer—at whatever level—is unclassified and unanalyzed; and

2. Neither the consumer nor the producer of intelligence has yet developed a capability for discovering, discriminating, distilling, and digesting *intelligence* within this overwhelming information environment replete with multiple sources of conflicting information.

Perhaps the most important aspect of Information Operations is the defensive aspect. Our highest priority, one we must undertake before attempting to influence others, is that of putting our own information commons in order. We must be able to assist and support our consumers with knowledge management concepts, doctrine, and capabilities, such that they can "make sense" of the information chaos surrounding them. This is perhaps most vital within the policy-making community.

Accepting the larger definition of Information Operations proposed in this paper, there are distinct benefits for each major constituency group:

- **Policymakers** will have significantly improved intelligence that fully appreciates cultural, economic and regional nuances not well covered by classified sources, and will have open-source intelligence products that can be readily shared with both home and host-country counterparts, press, and public.

- **Acquisition Managers** will be able to obtain strategic generalizations that accurately evaluate the threat in their respective mission areas at each level of analysis, while also establishing regional generalizations upon which to make sounder decisions about logistics and C4I supportability as well as countermeasure requirements.

- **Commanders and Staffs** will have access to unclassified open-source intelligence, including commercial imagery, that are essential to begin the contingency planning process, to execute humanitarian assistance operations, to guide classified collection management, and to place classified reporting in context. Open source intelligence will provide cover for communicating critical battlefield information to coalition and civilian partners including non-governmental organizations, and in general will provide for the common view of the battlefield or issue area essential to complex command and control. As will be noted in the section on global geospatial shortfalls, for this constituency group the most vital benefit is the ability of commercial imagery to address the 90% of the requirements for image maps that have not been met and will never be met by classified sources.

- **Publics** will have access to relatively straightforward and reliable explanations of foreign and domestic conditions and perceptions that are causing policymakers to take action, or requiring the acquisition of certain capabilities, or requiring the preparation of forces for employment. In the world of global information, the first three constituencies cannot rely on the media to do an accurate job of reporting; the public must receive a level of "intelligence support" which heretofore has not been necessary but which is now vital to the smooth transition from peace to war, or vital to reasonable popular understanding of particular crisis response options.

Net Assessments: An Operational View of Knowledge.

The acquisition community has a different sort of problem: the absence of an effective model for providing sophisticated threat assessments in relation to both the levels of analysis and the real-world conditions under which the systems are to be used.

Absent such a model, our intelligence analysts have no alternative but to continue doing what they do today: concluding that every threat is a "worst case" threat to be evaluated strictly on the basis of its maximum technical lethality, while avoiding coming to grips with generalizations about the environment which should, but do not, influence acquisition decisions.[13]

In fact, the threat changes in relation to both the level of analysis and the geographic-civil context within which friendly and enemy military capabilities are deployed (Figure 10). We will focus only on the first aspect here. Taking Libyan tanks in 1990 as an example:

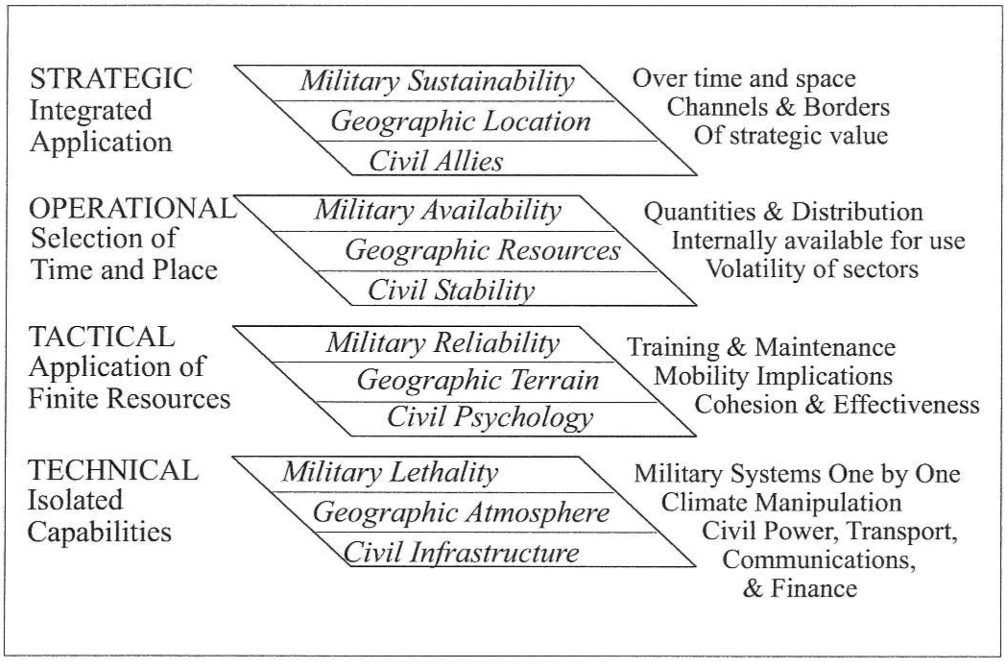

Figure 10. Net Assessment and Open Source Intelligence.

- At the technical level (lethality), since they are the best tanks that Soviet money can buy (at the time, the T-72), they must be evaluated as a very high threat. *This is where existing practices start and stop.*

- At the tactical level (reliability), once one appreciates the lack of training for the crews, the long-term storage of many of the tanks in the open, and the cannibalization of some tanks to keep others operational, the threat drops to low.

- At the operational level (availability), given the number of tanks scattered around, the threat rises to medium.

- At the strategic level (sustainability), the threat drops again to low for obvious reasons associated with both command and control and logistics supportability deficiencies.

The United States cannot pretend to have a viable Information Operations doctrine so long as this travesty of analytical impoverishment is allowed to continue. There is not a single intelligence report in existence today (nor available from the past) which reflects this level of sophistication and distinction, and that is something that must change soon. We continue to design and acquire systems in isolation from the real-world threat and the real-world environment in which they are to be employed. This robs the nation of scarce resources which could be applied much more effectively in other pursuits, including the pursuit of Information Peacekeeping Operations.

There is one other major deficiency in U.S. intelligence doctrine: its rather naïve focus on just three major areas of interest: the traditional two areas of political-military intelligence and scientific and technical intelligence; and the more recently activated area of economic intelligence. Despite the good efforts of some leaders in the past, notably Secretary of State Warren Christopher,[14] the United States continues to give short shrift to the critical intelligence challenges associated with sociological and ideo-cultural intelligence; demographic intelligence; and environmental intelligence. In order to plan and execute Information Operations that are precise and likely to have the desired outcome, the United States must radically expand its concepts and doctrine for national intelligence so as to be able to comprehend the full range of intelligence challenges across both domains of interest and nations of interest. It cannot do this if it relies primarily on the classified intelligence community and secret sources.

Information Peacekeeping: The Heart of Information Operations.

Information Peacekeeping is the active exploitation of information and information technology—in order to modify peacefully the balance of power between specific individuals and groups—so as to achieve national policy objectives. The three elements of Information Peacekeeping, in order of priority, are: open-source intelligence (providing useful actionable unclassified information); information technology (providing "tools for truth" that afford the recipient access to international information and the ability to communicate with others); and electronic security and counter-intelligence (a strictly defensive aspect of Information Operations). (See Figure 11.)

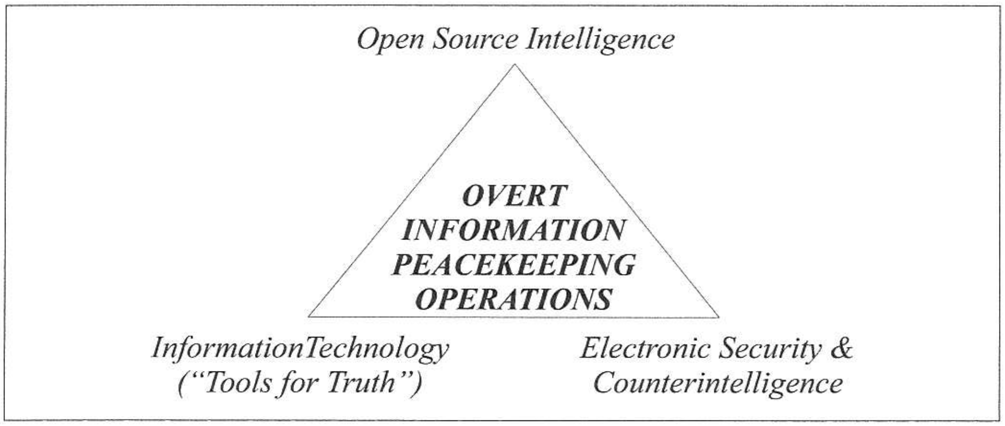
Open Source Intelligence
OVERT INFORMATION PEACEKEEPING OPERATIONS
InformationTechnology ("Tools for Truth")
Electronic Security & Counterintelligence

Figure 11. Elements of Overt Information Peacekeeping Operations.

To understand what this means, it is useful to specify what Information Peacekeeping is *not*. Information Peacekeeping is not:

- Application of information or information technology in support of conventional military peacekeeping operations, or in support of United Nations, coalition, or diplomatic operations.

- Development and execution of traditional psychological operations or deception operations that strive to manipulate perceptions in order to achieve surprise, or to cause actions to be taken that would not have been taken if the true circumstances were known.

- Covert action media placement operations, covert action agent of influence operations, or covert action paramilitary operations

- Clandestine human intelligence operations or overt research operations.

Although Information Peacekeeping is not to be confused with clandestine or covert methods, there are gray areas. Information Peacekeeping may require the clandestine delivery of classified or open source intelligence, or the covert delivery of "tools for truth" such as the traditional radio broadcast equipment, or the more recently popular cellular telephones and facsimile machines. Information Peacekeeping may also require covert assistance in establishing and practicing electronic security and counterintelligence in the face of host country censorship or interference.

On balance, then, Information Peacekeeping is by its nature most powerful and effective when it relies exclusively on open sources of information, the delivery of open-source intelligence, and on overt action. Under these conditions, it is incontestably legal and ethical under all applicable rules of law, including host country and non-Western cultural and religious rules of law and custom.

Information Peacekeeping is the tactical "force of first resort" for 21st century operations, and every theater and every major command, must have an order of battle able to conduct overt Information Peacekeeping Operations in all three of its major aspects.

Existing staff functions are not adequate to this challenge at this time. Taking each of the major staff elements for a theater command in turn:

- J-1 (Administrative). Generally includes handling of refugees and prisoners of war. No concepts, doctrine, or "order-of-battle" for treating information as either a munition or a critical logistics elements. Of most immediate concern: no J-1 (or G-1 or S-1) appears to have at hand an approved Table of Organization and/or Table of Equipment for handling humans who are placed under military care in a tactical environment.

- J-2 (Intelligence). Generally reactive and apathetic—takes whatever it can get from classified national intelligence systems. Does not have the concepts, doctrine, funding, security permissions, or "order-of-battle" for going out and getting open-source intelligence with which to provide direct support to theater operations.

- J-3 (Operations). Focuses strictly on placing munitions on target, positioning troops, and planning movements. Does not have concepts, doctrine, or an "order-of-battle" with which to use information as a substitute for munitions or men. Note that the execution of Information Warfare attacks, or the conduct of Psychological Operations, do not count and do not have the same effect as Information Peacekeeping Operations.

- J-4 (Logistics). Focuses on beans, bullets, and band-aids. Not responsible for evaluating or considering how full or empty the various constituencies are with respect to information essential to their mission. Imagine how effective a command might be if its information requirements—and those of its coalition partners and civilian agency counterparts—were treated with the same seriousness as fuel stocks or critical spare parts for fighter aircraft.

- J-5 (Plans/Other). Focuses on plans in isolation. Is not held accountable for declaring specific plans to be unsupportable due to a lack of intelligence or maps. The fact is that most theater contingency plans have made no provision for acquiring the necessary open-source intelligence—including commercial imagery—because everyone is assuming that national capabilities will suffice and will be made available. This is fiction.[15]

- J-6 (Communications). Focuses on administration of limited bandwidth and assignment of limited communications and computing resources, as well as subsequent oversight of the entire architecture. Is not held accountable for considering how the theater will communicate with coalition and civilian partners who are not equipped to U.S. standards. Is burdened by a vast and very expensive C4I architecture designed by the military services, all of whom assumed that the United States would always be fighting a unilateral military action in which all parties have the necessary clearances to be part of the largely classified theater command- and-control system. In particular, the J-6 is not held accountable for ensuring that externally acquired data, including maps, and external nodes, including non-governmental groups, can be fully integrated into the larger Information Operations environment within which the CINC must operate.

Others can focus on the information technology and electronic security aspects of Information Peacekeeping—this article will conclude with an examination of the most important aspect of Information Peacekeeping: the use of open source intelligence to understand, shape, and dominate the knowledge terrain in the "battle area."

Virtual Intelligence: The Brain of Information Operations.

In the words of Richard Kerr, speaking in late 1997: "The Intelligence Community has to get used to the fact that it no longer controls most of the information."[16] What this really means is that the United States can no longer rely exclusively on classified sources for the bulk of its intelligence, nor can the intelligence consumer communities—including the very important military operational and tactical consumers—assume that all of its intelligence needs will be met by the U.S. Intelligence Community as it has traditionally operated.

The Commission on Intelligence, a bi-partisan endeavor that included members appointed by both parties of the House and Senate, as well as members appointed by the Administration, offered two pertinent recommendations:[17]

- The U.S. Intelligence Community is "severely deficient" in its access to open sources, and this should be a "top priority" both for the attention of the Director of Central Intelligence and for funding.

- The consumers of intelligence should not refer requirements to the U.S. Intelligence Community when they can be answered predominantly through open sources, but rather should create their own open source intelligence.

- The Commission on Intelligence made these two recommendations because its investigations clearly documented that in the Information Age, the vast majority of usable, relevant information necessary to support policymakers, acquisition managers, and commanders is available in unclassified form from private sector sources—open sources are by definition sources which are legally and ethically available to anyone.[18]

The greatest obstacle to improved use of open sources is not that of *access*, which is freely or inexpensively available to all, but rather that of *acceptance*. The two most erroneous perceptions among experienced professionals who should know better are that open sources are "merely a collection of newspaper clippings" (in the words of a senior Intelligence Community official) or "the Internet" (in the words of a general officer). Figure 12 shows an illustrative, but by no means comprehensive, range of open sources, software, and services.

SOURCES	SOFTWARE	SERVICES
Current Awareness (e.g. Individual Inc.)	Internet Tools (e.g. NetOwl, Web Compass)	Online Search & Retrieval (e.g. NERAC, Burwell Enterprises)
Current Contents (e.g. ISI CC Online)	Data Entry Tools (e.g. Vista, BBN, SRA)	Media Monitoring (e.g. FBIS via NTIS, BBC)
Directories of Experts (e.g. Gale Research, TEL TECH)	Data Retrieval Tools (e.g. RetrievalWare, Calspan)	Document Retrieval (e.g. ISI Genuine Document)
Conference Proceedings (e.g. British Library, CISTI)	Automated Abstracting (e.g. NetOw., DR-LINK)	Human Abstracting (e.g. NFAIS Members)
Commercial Online Sources (e.g. LN, DIALOG, STN, ORBIT)	Automated Translation (e.g. SYSTRAN, SRA NTIS-JV)	Telephone Surveys (e.g. Risa Sacks Associates)
Risk Assessment Reports (e.g. Forecast, Political Risk)	Data Mining & Visualization (e.g. Visible Decisions, TASC Textor)	Private Investigations (e.g. Cognos, Pinkertons, Parvus)
Maps & Charts (e.g. East View Publications)	Desktop Publishing & Communications Tools	Market Research (e.g. SIS, Fuld, Kirk Tyson)
Commerical Imagery (e.g. SPOT, Radarsat, Autometric)	Electronic Security Tools (e.g. SSI, PGP, IBM Crytolopes)	Strategic Forecasting (e.g. Oxford Analytics)

Figure 12. Illustrative Range of Open Source Niches.

Also to be noted is the distinction between those resources which are readily available within the U.S. Intelligence Community; within the rest of the government; within the nation (i.e., in the private sector with its universities, information brokers, businesses, media, and other information activities); and within the larger global information community. It is absolutely essential that each intelligence producer and consumer have a "map" of this larger knowledge terrain, and a strategy for assuring their ability to discover, discriminate, distill, and digest critical open-source information and intelligence.

Those familiar with the existing security and procurement practices of both the U.S. Intelligence Community and the military operations environment will recognize that there are enormous obstacles to progress in this area. An ignorance of what is available in the private sector and a reluctance to reveal our rather obvious interests cause many to eschew the benefits of open-source intelligence. Simultaneously, our procurement system is biased in favor of multi-million dollar contracts with beltway bandits whose expertise is largely in how to win procurements that focus predominantly on providing technology solutions, rather than the direct ability to harness world-class expertise. We must move rapidly toward a more open intelligence environment in which individual analysts and individual desk officers are empowered with the knowledge and the procurement authority to obtain "just enough, just in time" open source information and intelligence support.[19]

Geospatial Gaps: The Achilles' Heel of Information Operations.

In the over-all scheme of information operations, there is no greater debility than the almost total lack of global geospatial mapping data at a scale of 1:50,000.

- This is the level necessary for tactical movement of troops under fire, for the coordination of combined-arms support, for the targeting of precision munitions, and for the simulation of three-dimensional nape-of-the-earth approaches for sensitive aviation missions.

- It is also the level at which automated all-source data fusion (the Holy Grail for all intelligence technocrats) and automated multi-source data visualization become "real."

The National Imagery and Mapping Agency (NIMA) acknowledges that it has less than 10% of the world at this level, and has no plans for acquiring commercial imagery in order to create a global geospatial database at this level.[20] As the Defense Mapping Agency (DMA) discovered during the Gulf War, NIMA is also incapable of creating 1:50,000 maps—even with full support from commercial imagery sources—in less than 60-90 days.[21]

The broad nature of the deficiency can be defined as follows:

- For Africa, where many of our unexpected contingencies occur, we do not have acceptable mapping data for 13 countries including Ethiopia, South Africa, and Uganda.

- For Asia and the Pacific, an area many consider central to our economic future and also highly subject to regional disturbances, we do not have acceptable mapping data for 12 countries, including China, Indonesia, and Papua New Guinea, nor for the four major island groups including the contested Spratly Islands.

- For Europe and the Mediterranean, Greece and Turkey remain completely uncovered, despite their importance to NATO, their traditional rivalry, and the role of Turkey in relation to the former Soviet Republics, Iraq, and Iran.

- For the Western Hemisphere, our own "back yard," we lack acceptable mapping data for 13 countries, including Argentina, Colombia, Mexico, and Paraguay.

This deficiency will continue to exist for the next decade or two—and beyond—unless there is a deliberate decision made at the Presidential level, with full support from the Joint Chiefs of Staff, to resolve this deficiency immediately. The cost for resolving it has been estimated by knowledgeable senior leaders of NIMA at between $250 million and $500 million a year in commercial imagery procurement for the next five to six years.[22] This cost would cover, among other important projects, complete 1:50,000 coverage of China, the Amazon, and Africa. In combination with the planned shuttle mission in 2002 to collect precision points (Digital Terrain Elevation Data) for the entire Earth, this will allow the United States to have a phenomenal intelligence and Information Operations advantage, as the only country in the world with a complete accurate map of every significant portion of the Earth at the 1:50,000 scale.

In the absence of such geospatial data at the 1:50,000 level, policy options are severely constrained. Precision munitions cannot be used until the imagery and mapping data are collected and processed; Special Operations units and drug interdiction teams are at a major disadvantage; conventional military and law enforcement operations cannot be properly planned and executed; humanitarian assistance and other coalition operations are handicapped—the list goes on and on.

There is no one today, at any level of the military and certainly not within the White House or any other Cabinet department, who is willing and able to make this case before the Secretary of Defense and the President of the United States—hence we continue to plan for the future with our "eyes wide shut."[23.]

Conclusion: New Doctrine for a New Era.

Information Peacekeeping is in effect both a strategy for government operations and a national security strategy with global reach; consequently it has profound implications for *how we train, equip, and organize our government and our military* (Figure 13).

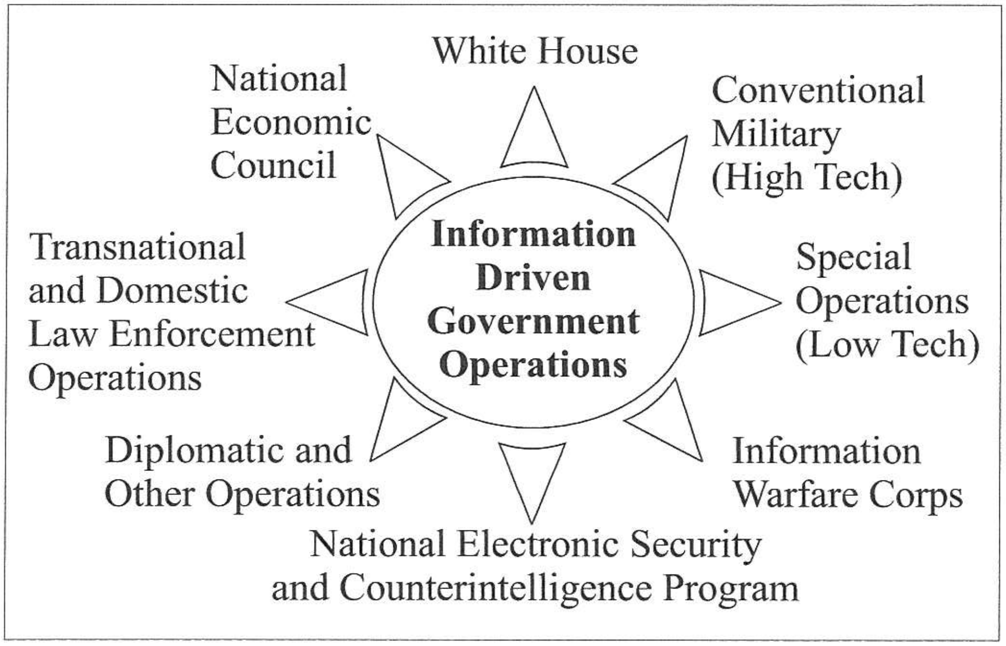
White House
Conventional Military (High Tech)
Special Operations (Low Tech)
Information Warfare Corps
National Electronic Security and Counterintelligence Program
Diplomatic and Other Operations
Transnational and Domestic Law Enforcement Operations
National Economic Council
Information Driven Government Operations

Figure 13. New Government Operations Doctrine.

In the final analysis, we must come to grips with the fact that our government today is an industrial-era government, woefully inadequate in all respects as to the management of internal information and the acquisition and exploitation of external information. This in turn renders us wastefully ineffective in the planning and execution of global influence operations, both those that use information and those that use violence or other means.[24]

We can, however, remedy this situation. The following steps are recommended:

1. Provide the Director of Central Intelligence with the centralized program management authority over all classified collection and production programs, as envisioned in the National Security Act of 1992 (which was not adopted by Congress).[25]

2. Create a new Director of National Intelligence within the existing National Security Council (NSC) structure,

responsible for oversight of government information operations from a substantive point of view.

a. Elevate the National Intelligence Council by moving it to this new office, and expand it modestly by creating National Intelligence Officers corresponding to each of the major consumer groups in government and in the private sector. The existing geo-functional NIO's would become Associate NIOs and would continue to serve as the focal points for regional and topical intelligence management.

b. Provide $1 billion a year for a Global Knowledge Foundation, modeled after the National Science Foundation, but responsible for nurturing (but not regulating or overseeing) distributed centers of expertise world-wide, all of which can comprise the "Virtual Intelligence Community," or, in traditional terms, a truly *national* intelligence reserve.

c. Subordinate both classified intelligence and Departmental intelligence endeavors to a larger national intelligence community that uses open sources of intelligence as the source of first resort,[26] while restoring the classified intelligence community to its rightful place as the source of *last resort*, authorized to use whatever means necessary to acquire critical information *not available through other means*. Fence the existing classified budgets for a decade, specifically precluding the Secretary of Defense from reducing those portions of the intelligence budget concealed within Department of Defense budget lines.

d. Subordinate the existing Electronic Security and Counter-intelligence Program, for which funding on the order of $1 billion a year has been recommended by the President's Commission on Critical Infrastructure Protection, to this larger office, but leave executive authority for its execution with the Federal Bureau of Investigation. This is essential, because the "Virtual Intelligence Community" cannot exist without national electronic security and counter-intelligence guarantees to the private sector.

Among the first steps a new Director of National Intelligence might take would be:

1. Establish a National Net Assessments Center to apply net assessment methods to domestic issues as well as non-military international issues. The existing military Net Assessments Office could, with some significant changes in focus and the integration of representatives from the other Departments of government, serve as the cadre for this broader national center.

2. Establish a National Open-Source Consortium to transfer knowledge of open sources, software, and services to all levels of government, as well as all elements of the private sector.

3. Establish four small Threat Assessment Centers corresponding to each of the four warrior classes, and modeled after the DCI Centers now in existence for terrorism and "crime and narcotics," but with a major emphasis on the collection and exploitation of open sources. Alternatively, these could be small five-person oversight cells within the office of the DNI/NSC.

4. Establish a commercial imagery fund able to procure, at substantial discounts, all commercial imagery needed by the civilian departments, the military, law enforcement, and the NATO/Partners for Peace program.[27] Rather than entrust NIMA with these funds (NIMA may not be around in the near future), the funds would be maintained by the DNI and allocated to the CINCs and Departments for expenditure as they each deem appropriate.

5. Establish a Presidential Commission on National Intelligence to examine how best to create an integrated information "order-of-battle" which fully harnesses the knowledge and information management skills of both the federal and state governments, and the private sector. The Commission would have as a specific objective defining a

new national intelligence reserve concept that facilitates the inclusion of civilian experts (including international experts), on an "as needed" basis.

Finally, then, we come to "who cares?" and "why should we?" What do we gain? We gain a swift, smart, sleek government able to provide for a "360°" or—in more modern terms—a "spherical"[28] defense at home and abroad, with revolutionary improvements in both our ability to influence others, and our ability to spend money wisely—fewer "hangar queens" and more "just right" stilettos. If we do not do this, if we continue to muddle through, then low-tech brutes will continue to slip through our crude defenses, low-tech seers will continue to be invisible to our warning networks, and high-tech seers will spend the next 20 years freely practicing information terrorism and vandalism, or plundering our electronic intellectual property and digital storehouses of wealth.

Only DoD has the mix of talent, resources, and influence to make the necessary things happen, and only DoD has the budget flexibility to permit realignment of the needed funds. It is *not* only DoD that must defend our nation from all enemies, domestic and foreign—this responsibility must fall evenly on every element of the government, including state and local governments. It *is*, however, DoD that must first rise to the challenge and lead us to a thinking about, and funding, a future where Information Peacekeeping is recognized as the purest form of war, and the only path to sustained peace and prosperity.

ENDNOTES

1. Overemphasis on expensive and narrowly focused technical collection has been a consistent concern in every major review of the U.S. Intelligence Community since technical solutions came into vogue in the 1960's. For a fine summary of the "Seven Sins of Strategic Intelligence" identified by the Church Commission in 1975, see the article by Dr. Loch Johnson, in *World Affairs*, Fall 1983. Dr. Johnson's many books, including his most recent, *Secret Agencies: U.S. Intelligence in a Hostile World*, Yale, 1996, stand as one of the more

balanced collections of commentary on this important topic. This theme is repeated in the two major reviews completed recently within the U.S. Government, the first in *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, March 1, 1996; the second in *IC21: Intelligence Community in the 21st Century*, Staff Study, House Permanent Select Committee on Intelligence, March 4, 1996. According to authoritative senior officers, we process less than 10 percent of what we collect on both the imagery and the signals sides of the technical collection function. Of the various major reviews conducted in the mid-1990s, *In From the Cold: The Report of the Twentieth Century Fund Task Force on the Future of U.S. Intelligence*, 20th Century Fund Press, 1996, focuses most carefully on the urgent need for greater funding and quality control in all-source analysis. Mr. Mort Zuckerman and Mr. Richard Kerr were among the active contributors to this report. See also the background papers by Allan E. Goodman, Gregory F. Treverton, and Philip Zelikow.

2. In 1994 the author was invited by the National Research Council, affiliated with the National Science Foundation, to provide a review of the U.S. Army's multi-billion dollar multi-media communications plan for the future. The plan provided billions for internally-generated data, and nothing at all for acquiring the 80 percent of the information needed by the commander from external open sources, including commercial imagery. The plan also provided nothing for communicating with coalition partners, whose radios and typewriters remain incompatible with space-age communications and computing technologies.

3. The four warrior classes are discussed in detail in "The Transformation of War and the Future of the Corps," in *Intelligence Selected Readings—Book One*, U.S. Marine Corps Command and Staff College, AY 92-93.

4. See specifically Alvin Toffler, *PowerShift: Knowledge, Wealth, and Violence at the Edge of the 21st Century*, Bantam, 1990; and Alvin and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century*, Little, Brown, 1993.

5. One of the most intelligent and revolutionary writings pertinent to military doctrine is Martin J. Libicki, *The Mesh and the Net: Speculations on Armed Conflict in a Time of Free Silicon*, National Defense University Press, 1994.

6. Schwartau's first book, *Terminal Compromise*, was considered by his lawyers to be so controversial that he was required to publish it as a novel. His follow-on, *Information Warfare: Chaos on the Electronic*

Superhighway, Thunders Mouth Press, 1994, set the stage for global discussion and is widely credited with awakening both the international press and the international military to this critical issue area.

7. EAGLE VISION/JOINT VISION is a ground station transportable in a single C-130 that is capable of taking real-time feeds from both SPOT IMAGE, 10 meter, satellites and national satellites. Today it can feed directly into aviation mission rehearsal systems and allow interactive three-dimensional fly-through practice. If the Army will pay attention and hook up its 18-wheeler topographic vans to one of these ground stations, it can produce 1:50,000 combat charts with contour lines on a "just enough, just in time" basis. As tactical capabilities to exploit commercial imagery expand, it will be increasingly difficult for NIMA and the NRO to justify their existing budgets and production costs.

8. The author coined this term in 1994 in discussion with Mr. James Q. Roberts, Director for Psychological Operations in the Office of the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict. Subsequently the author prepared the paper "Information Peacekeeping: Innovative Policy Options," for the Assistant Secretary of Defense, Special Operations and Low Intensity Conflict, presented at OSS '96, September 18, 1996.

9. "The acme of skill is to defeat the enemy without fighting." This widely-accepted mantra has not yet influenced how we structure our military force packages.

10. Lee Felsenstein of the Interval Research Corporation is the originator of the term "information commons."

11. Over the years authoritative speakers including Mr. Ward Elcock, Director of the Canadian Security and Intelligence Service; Dr. Gordon Oehler, then Director of the DCI's Non-Proliferation Center, and many others have generally agreed that even for topics as seemingly difficult as terrorism and proliferation, open sources of information comprise roughly 80 percent of all-source solution. In fact open sources can contribute as little as 10-20 percent, mostly targeting assistance for denied area coverage by classified sources, and as much as 95-99 percent, strategic economic intelligence. The official National Foreign Intelligence Board finding, based on input from the Community Open Source Program Office, COSPO, is that the U.S. Intelligence Community, and most specifically the Central Intelligence Agency, spends 1 percent of its total budget on open sources, and for this amount of money receives 40 percent of its input to the all-source process.

12. This chart is adapted from materials developed by Dr. Jack Davis, recently retired ean of the Centray Intelligence Agency analysts, whose course, "Intellience Successes and Failures," was the model for the Harvard Intelligence Policy Seminar. A longer discussion of influences on the policymaker and obstacles to informed analysis and informed consumption is available in the author's "A Critical Evaluation of U.S National Intelligence Capabilities," *International Journal of Intelligence and Counterintelligence*, Summer 1993.

13. The author was Special Assistant and Deputy Director of the USMC Intelligence Center from its inception in 1987 through 1992. Early on the author worked with a team to define the Marine Corps model for analysis. A copy of the model, and of the strategic generalizations resulting from the model applied to 69 countries of interest to the Marine Corps, is available in *Open Source Intelligence Handbook*, Joint Military Intelligence Training Center, October 1996. The over-all process has been described in "Intelligence Support to Expeditionary Planners," *Marine Corps Gazette*, September 1991.

14. In his final year as Secretary of State, Warren Christopher unequivocally elevated the environment to the high table of national security. Undersecretary of State Wirth was influential in this matter, principally through the EARTHMAP Report in October 1995, an inter-agency endeavor of over a year's duration which concluded that sustainable development and many other key U.S. policies required accurate global geospatial data for the entire planet. Secretary Christopher was following in the footsteps of Secretary of State James Baker, who noted in his 1989 confirmation hearings the urgent need to increase emphasis on the environment.

15. General Phil Nuber, then Director of the Defense Mapping Agency, attempted—without lasting success—to get the theater commanders to evaluate their contingency plans using the established C-1 to C-4 status reporting system. Most theaters would get a failing grade on most plans because they are not being held accountable for planning the future supply of information and maps in the same way that they must plan for men, materiel, and munitions.

16. Mr. Kerr, former Deputy Director of Central Intelligence and former Director of Intelligence for the CIA, was speaking at OSS '97, "Global Security & Global Competitiveness: Open Source Solutions," in Washington, DC, on September 5, 1997.

17. *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, March 1, 1996.

18. The author was one of four people testifying to the Commission on open-source options. At the end of the day, a Thursday, the author was invited to participate in an exercise now known as "the Burundi Exercise," in which all available information from the U.S. Intelligence Community on Burundi was compared with what the author was able to mobilize from private sector sources over the week-end. At 10:00 a.m. on the following Monday, the Commission had received:

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

- **From Jane's Information Group,** a map of Burundi showing the tribal areas of influence; a 1-page order of battle for each tribe; and a volume of one-paragraph summaries with citations for all articles about Burundi published in the past couple of years in *Jane's Intelligence Review*, *International Defense Review*, and *Jane's Defense Weekly*.

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

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

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

- **From SPOT Image Corporation, USA,** it was determined that SPOT could provide digital imagery for 100 percent of Burundi, cloud-free and less than 3 years old, at a 10-meter resolution adequate for creating military maps with contour lines at the 1:50,000 level as well as precision-munitions guidance packages and nape of the earth interactive aviation and ground mission rehearsal simulation packages.

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

19. The Website http://www.oss.net offers the public, at no cost, over 5,000 pages from over 500 authorities that have spoken at the six previous open source intelligence conferences sponsored by the author. Included at this site are abridged versions of the Open Source Intelligence Handbook, the Open Source Intelligence Reader, and eight formal lessons on open source intelligence.

20. Based on official NIMA briefings at the unclassified level.

21. As was widely discussed in official circles at the time, General Nuber had to make a personal appeal to General Norman Schwarzkopf for realignment of national imagery assets to collect precision points with which to make maps. At the same time, the U.S. Air Force gave up on national imagery as its main source of wide-area surveillance and targeting imagery, and began buying vast quantities of commercial imagery directly—without DMA assistance or coordination.

22. Mr. Doug Smith, Deputy Director of NIMA, stated in 1996, at the fifth international symposium on "Global Security & Global Competitiveness: Open Source Solutions," that an estimate of $250 million a year was on the mark. In 1997 he revised this estimate upward toward $500 million a year. Despite his best efforts, however, neither DoD leadership nor the Executive Office of the President are willing to address this critical deficiency—and NIMA as a body has gone so far as to stonewall the *EARTHMAP Report* of October 1995 in which Undersecretary of State Wirth, among other leaders of the civilian elements of government, called for rapidly acquiring global geospatial data at this level of accuracy and detail. The obstacles appear to be twofold: a real ignorance at the theater level about the utility of existing SPOT IMAGE capabilities, and a real reluctance by the Office of the Secretary of Defense to buy commercial imagery from a French source—which prefers instead to wait for the constantly postponed offering of U.S. commercial imagery at the one-meter level of resolution (the author believes this will not be available to the degree SPOT IMAGE data is until about 2010). At the same time, everyone except EAGLE VISION aficionados continues to ignore the fact that one-meter imagery comes with enormous bandwidth, storage, time of

transmission, and cost burdens which we cannot afford in the foreseeable future. One-meter is a "designer" image option, not an industrial image option.

23. "Eyes Wide Shut" was the editorially assigned title for an article about this matter in *WIRED Magazine*, August 1997. The author's complete views on this grave deficiency were articulated in a presentation to the Third Congress of the North American Remote Sensing Industries Association titled "Exploring the Four Pillars: Government, Community, Market, and the World," Washington, DC, May 22, 1997. A copy of the speech outline is available at http://www.oss.net under Documentation/Speeches.

24. Paul Strassmann, former Director of Defense Information and former Chief Information Officer of the Xerox Corporation, among others, has published widely in the information management arena. He estimated that $22 billion could be saved over 7 years by instituting improved management of legacy and new systems. The author estimates that an equal or greater savings could be achieved by similar reforms on the content side—reforms intended to lead to more informed policy-making, acquisition management, and command planning.

25. "The National Security Act of 1992," *American Intelligence Journal,* Winter/Spring 1992, provides a side by side comparison of the changes recommended by the House and the Senate.

26. Mr. Paul Walner, the first Open Source Coordinator for the DCI, coined this term, and intended to emphasize what the Commission on Intelligence subsequently endorsed: that classified capabilities should be called upon only when the intelligence needed cannot be obtained by other means—through open sources.

27. The formal internal paper now in circulation with UK MOD is titled "Proposals for the Development of an Open Source Programme to Support NATO and PfP Activities." The author, Captain Patrick Tyrrell, British Royal Navy, now serves as Commandant of the Defence Intelligence and Security School. Captain Tyrrell earned his OBE for work with NATO leadership, and has an intimate understanding of NATO operational and intelligence capabilities and requirements in relation to the Partners for Peace.

28. Mr. Douglas Dearth has coined this latter term, with the intent of emphasizing that the traditional term is one-dimensional, on a single plane.