INFORMATION OPERATIONS: PUTTING THE "I" BACK INTO DIME

Robert David Steele

February 2006

*****

The views expressed in this report are those of the author and do not necessarily reflect the official policy or position of the Department of the Army, the Department of Defense, or the U.S. Government. This report is cleared for public release; distribution is unlimited.

*****

Comments pertaining to this report are invited and should be forwarded to: Director, Strategic Studies Institute, U.S. Army War College, 122 Forbes Ave, Carlisle, PA 17013-5244.

*****

All Strategic Studies Institute (SSI) monographs are available on the SSI homepage for electronic dissemination. Hard copies of this report also may be ordered from our homepage. SSI's homepage address is: *www.Strategic Studies Institute.army.mil*.

*****

The Strategic Studies Institute publishes a monthly e-mail newsletter to update the national security community on the research of our analysts, recent and forthcoming publications, and upcoming conferences sponsored by the Institute. Each newsletter also provides a strategic commentary by one of our research analysts. If you are interested in receiving this newsletter, please subscribe on our homepage at *www.Strategic Studies Institute.army.mil/newsletter/newsletter.cfm*.

ISBN 1-58487-228-4

CONTENTS

FOREWORD

The Department of Defense (DoD) has made major strides in the development of concepts and doctrine for Information Operations (IO). In a substantive break with past traditions, the Secretary of Defense has made the U.S. Strategic Command (USSTRATCOM) and the U.S. Special Operations Command (USSOCOM) supported commands rather than supporting commands. USSTRATCOM has the national mission and is taking the lead in IO. USSOCOM has the national mission and is taking the lead in the Global War on Terror (GWOT). Across all other Combatant Commands, and within all services and agencies of DoD, the Undersecretary of Defense for Intelligence (USDI) is sponsoring transformative leap-ahead endeavors in Strategic Communication, Open Source Intelligence (OSINT), and Joint Intelligence Operations Commands or Centers (JIOC) focused on interagency and interservice information-sharing and collaboration.

This monograph offers an overview of the operational and information challenges that face DoD, describes six "IO-heavy" mission areas, goes on to outline a detailed strategic concept of operations, and ends with a requirements statement, intended to be helpful to every COCOM, service, and agency. As the author suggests, IO can be viewed from a content perspective as having three ingredients: Strategic Communication (the message), OSINT (the reality), and JIOC (the technology). By clearly addressing global monitoring in all languages, 24/7; integration of a global man-machine foreign language translation network; and exploitation of leap-ahead deep web data mining and predictive analysis softwares—the author is defining "best practices" helpful to DoD. The Strategic Studies Institute hopes that this monograph will stimulate a better understanding of modern IO.

DOUGLAS C. LOVELACE, JR.
Director
Strategic Studies Institute

SUMMARY

The end of the Cold War and the emergence of terrorism; radicalized religion; the proliferation and commoditization of weapons of mass destruction (WMD); and the increased informational and economic power of Arabia, Brazil, China, India, Indonesia, Iran, Russia, and Venezuela, among others, have brought Information Operations (IO) to the forefront of the unified national security strategy.

In the past year, IO has matured from an early emphasis on the protection of critical infrastructures and against electronic espionage, and is now more focused on content and on interagency information-sharing. The value of information—all information, not only secret information—and the value of global monitoring in all languages, 24/7, have been clearly established by the Undersecretary of Defense for Intelligence (USDI).

This monograph defines and discusses three IO elements:

- Strategic Communication (the message);
- Open Source Intelligence (the reality); and,
- Joint Information Operations Centers (the technology).

These elements are further discussed in relation to six "IO-heavy" mission areas:

- Information Operations generally;
- Peacekeeping Intelligence (reactive);
- Information Peacekeeping (proactive);
- Early Warning (conflict deterrence, proactive counterterrorism);
- Stabilization and Reconstruction Operations; and,
- Homeland Defense and Civil Support.

The monograph concludes with a strategic overview of the various conceptual and technical elements required to meet modern IO needs, and provides a requirements statement that could be tailored to the needs of any Combatant Commander, service, or agency.

Recommendations.

Executive. The creation of a National Information Council (NIC), coequal to the National Security Council (NSC) and the National Economic Council (NEC), is necessary if the White House is to both harness the distributed intelligence of the nation and the world, and also achieve its objectives in public diplomacy, strategic communication, interagency information-sharing and collaboration, the renaissance in public education, and the resurrection of national research.

Congress. Intelligence and information-sharing are inherent critical aspects of all government operations. Each congressional committee should create a Subcommittee on Intelligence and Information Operations (I2O). The chair and ranking minority member of each of these subcommittees, or their designated representatives, should in turn comprise a new Special Committee on I2O that has oversight over the national Open Source Agency, information operations across all federal agencies, and a special relationship with the respective Intelligence Committee, which shall continue to focus on classified sources and methods.

White House. Expand the extraordinary Earth Science information-sharing initiative to include the sharing of information about disease, crime, poverty, and other nontraditional threats to our national security and prosperity.

Director of National Intelligence. Free the Open Source Agency (OSA) from U.S. intelligence community affiliation or direct oversight. Instead, follow the expert recommendation that it be a sister agency to the Broadcasting Board of Governors under Department of State auspices. Fully fund the Open Source Information System–External (OSIS-X) as a commercial venture open to all legitimate governments; nongovernmental organizations; and private sector corporations, universities, and groups.

Department of State. Establish an Office for Information-Sharing Treaties and Agreements. This small office of perhaps 10 individuals, led by accredited diplomats, would negotiate information-sharing treaties with nations and information-sharing agreements with organizations, with the immediate objective of extending data and information standards to all participants. Integrate all Embassies into information-sharing mode.

Department of Defense. Rapidly establish JIOCs within each Combatant Command (COCOM) as well as a DoD JIOC, while establishing two new Combatant Commands: one for I2O, and one for Stabilization & Reconstruction. Integrate the Strategic Decision Support Center envisioned by Captain Scott Philpott, USN, into COCOM I2O. Redirect the U.S. Strategic Command (USSTRATCOM) toward the oversight and orchestration of Big War. COCOM I2O should have oversight of the Defense Information Systems Agency (DISA), Defense Technical Information Service (DTIC), and the varied Departmental-level intelligence organizations as well as authority over the JIOCs at each COCOM similar to that retained by the services over ground, sea, and air components. Deliberately attend to the I2O needs of policy, acquisitions, logistics, and operations with OSINT as the source of first resort (always copied simultaneously to the relevant all-source intelligence provider). Place the National Guard under the operational oversight of the U.S. Northern Command (USNORTHCOM), and begin the process of redirecting the Guard toward a true Home Guard role in which they have specialized units for medical, fire, police, and disaster-relief engineering that are equally suitable for homeland security duties as well as support for global stabilization and reconstruction operations.

General Services Administration (Office of Intergovernmental Solutions). Sponsor a summit and an ongoing Wiki web site on the four "opens" that will energize information-sharing in the future:

a. Open Source Software

b. Open Source Information

c. Open (Electromagnetic) Spectrum

d. Open Hyperdocument System (OHS)

Department of Commerce. Issue an antitrust waiver for a private sector OSINT skunkworks that will fully integrate and test all avail-able open sources, softwares, and services. This will do for IO/OSINT what the Microelectronics and Computer Technology Corporation (MCC) initative sought to do for artificial intelligence under Admiral Bobby Inman. This skunkworks will accelerate the development of open common standards for information-sharing that will be truly worldwide, with the added advantage of developing

commercial alternatives for the sharing of secret information across national, cultural, and government to nongovernment boundaries on a by-name, by-paragraph basis.

Department of Justice. Propose to Congress legislation that would mandate the open disclosure and stability of Application Program Interfaces (API) within all software purchased by the government and offered for sale within the United States. API are the equivalent in cyberspace of a common railway guage such as was required to make national rail a reality. Demand that all software have transparent stable API by 2008, or be banned from the Federal marketplace.

Open Source Agency. Execute the 100-day start-up plan, which (already drafted) is easily doable by drawing on the OSINT pioneers across the U.S. Army and in other services. The plan includes:

1. IO/OSINT training program employing resident, mobile, and remote learning
2. IO/OSINT help desk, 24/7, multi-lingual
3. IO/OSINT global translation web in all languages that will support 911 calls
4. IO/OSINT historical and cultural "Manhattan Project"
5. OSIS-X with DoD first, then NATO, then each COCOM's coalition partners
6. OSIS-X free access to all NGOs and academic institutions
7. Create a living directory of top 100 experts on each country and topic.
8. Create Texas Early Warning Center
9. Create New York Corporate Warning Network
10. Digital Marshall Plan using residual capability in abandoned satellites
11. Subsidize the Security Affairs Support Association (SASA) in developing executive seminars in information-sharing and intellectual property management—then create the University of the Republic as a fee-based means of fostering information-sharing across organizational boundaries.

U.S. Army and U.S. Marine Corps. Focus on recruiting, training, and nurturing an Army and a Marine Corps of self-starters, each able to master at least one foreign language, each able to master Eastern fieldcraft, stealth, and patience, and each able to leverage their innate intelligence, communicated intelligence, information superiority, interagency planning and operations, and precision delivery of water, food, medicine, and munitions where required, in order to stabilize and reconstruct any environment, at home or abroad. It is brainpower, not firepower, which will win the 100-year six-front war upon which we are now engaged.

U.S Navy and U.S. Air Force. Focus on creating a 450-ship Navy capable of global distributed operations in littoral waters, and on being able to carry out two Berlin Airlifts simultaneously, one with organic air and one with conscripted air. Speed of presence, triggered by early warning, not massed fires over time, is what matters now.

U.S. Public. You may not be interested in war, but war is interested in you. We are at total war. Thomas Jefferson had it right: "A Nation's best defense is an educated citizenry." IO and OSINT, at root, are about educating and legally and ethically engaging every person of good will in the honorable tasks of protecting our nation and enhancing our prosperity.

CHAPTER 1

INTRODUCTION

The end of the Cold War and the emergence of terrorism; radicalized religion; the proliferation and commoditization of weapons of mass destruction (WMD); and the increased informational and economic power of Arabia, Brazil, China, India, Indonesia, Iran, Russia, and Venezuela, among others, have brought Information Operations (IO) to the forefront of the unified national security strategy.[2] The administration and Congress both recognize that strategic communication, public diplomacy, and interagency information-sharing and collaboration must be core competencies within a transformed national security arena. Robust interagency information-sharing and collaboration practices will be most effective if there is a common understanding of the real world based on global foreign information acquisition and analysis. This monograph offers a campaign plan for meeting the requirements established by the Undersecretary of Defense for Intelligence (USDI) in January 2004: universal coverage, 24/7, waged in all languages, extending down to the tribal and neighborhood levels of granularity.[3] This proposed capability addresses the specific needs of the U.S. Strategic Command (STRATCOM), the U.S. Special Operations Command (SOCOM), and the regional Combatant Commanders (COCOM) and their supporting elements including the services. It also provides for rapid inexpensive replication across all federal, state, and local elements associated with homeland security or national security, and for rapid inexpensive migration to coalition governments and nongovernmental organizations that agree to enter into information-sharing treaties or information-sharing agreements with the Department of Defense (DoD).

In the Age of Information, the primary source of national power is information that has been converted into actionable intelligence or usable knowledge. According to Alvin and Heidi Toffler, "Knowledge—in principle inexhaustible—is the ultimate substitute."[4] In their book, *PowerShift*, the Tofflers go on to discuss knowledge as a substitute for wealth, for natural resources, for energy, for violence,[5] and even for time and for space. Knowledge—

the vast majority of which is not classified—is the ultimate source of national power.

It is for this reason that Undersecretary of Defense for Intelligence (USDI) Dr. Stephen A. Cambone is "on point" when he demands as his primary objective for Defense information and intelligence: "universal coverage, 24/7, in all languages in near-real-time, at sub-state levels of granularity."[6] This transformative vision was validated by the Defense Science Board in two seminal studies, *Strategic Communication* (July 2004), and *Transitions to and from Hostilities* (December 2004).[7]

Achievement of this well-chosen set of objectives demands three separate transformative Information Operations (IO) campaigns, each integrated and extendable down to the state and local levels for Homeland Defense, and also transferable externally to nongovernment (NGO) and other organizations controlling the 90 percent of information that will never be readily available to classified agencies:[8]

> Information-Sharing: the creation of joint interagency information-sharing and collaboration networks and centers whose capabilities can be replicated quickly and *inexpensively* by, among others, homeland security elements including states and counties, NGOs, universities, and coalition partners.[9] This capability ensures that what we already know, or what our allies already know, can be readily shared with all concerned.
>
> Global Monitoring: the establishment of a mission-oriented global information monitoring system that can master the full spectrum of available information in all languages[10] and that is both tailored to defense needs and responsive to operational tempo (i.e. effective in near-real-time).
>
> Translation: the establishment of a man-machine foreign language translation network that can collect, process, and exploit foreign language information, both written and verbal, in real-time, at the tactical, operational, and technical levels.[11]

This monograph outlines how we might integrate three IO elements—Strategic Communication (the message), open Source Intelligence (the reality), and, Joint Intelligence Operations Centers (the technology)[12]—in support of six distinct "IO-heavy" operational missions:

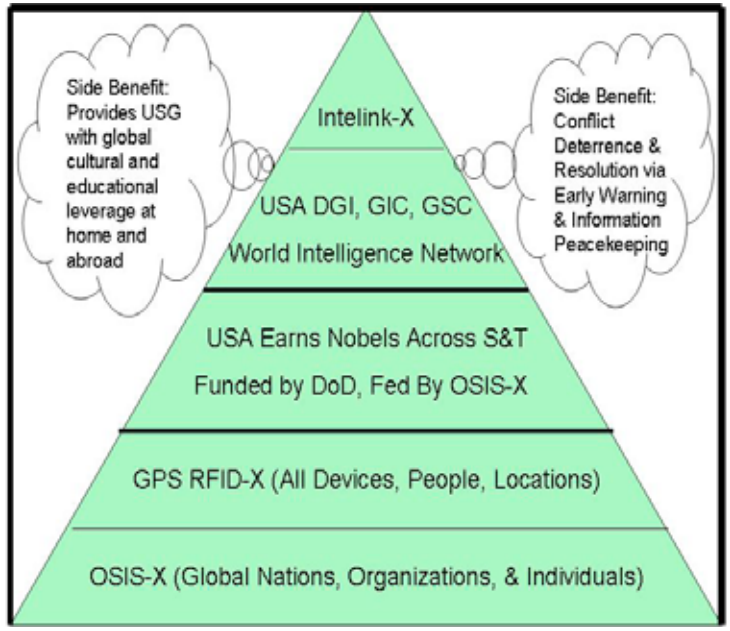
- Information Operations,
- Peacekeeping Intelligence (reactive),
- Information Peacekeeping (proactive, preventive),
- Early Warning (conflict deterrence, proactive counterterrorism),
- Stabilization and Reconstruction Operations, and
- Homeland Defense and Civil Support.

Concurrently we must also revitalize national education and national research in tandem with the *foundation* of national power in the Age of Information.

It is imperative that DoD integrate the design, funding, and management of all three IO elements into one coherent whole. Addressing any one of them in isolation is a prescription for failure.[13] It is also imperative that we follow the USSOCOM lead and recognize that finished secret intelligence is a fraction of the secret information available to us, and that all raw information—secret, unclassified, operational, logistic—must be brought together across distributed "pits" that are able to share all relevant information with one another.

Figure 1 shows an advance view of this monograph's concluding illustration. The monograph will explain why it will be helpful to DoD IO.

Modern IO is not about the old messages of psychological operations (PSYOPS), but rather about empowering billions of people with both information tools and access to truthful information. It is about education, not manipulation. It is about sharing, not secrecy. It is about human understanding to create wealth and stabilize societies, not about the threat of violence and the delivery of precision munitions. IO substitutes information for violence.



DGI: Director of Global Information GIC: Global Intelligence Council GSC: Global Strategy Council

Figure 1. Creating the World Brain for U.S. Benefit.

OPERATIONAL CHALLENGES

Information Operations.

Although the classified world has been aware of the vulnerability of electronic communications and computing systems for decades, and some extraordinary intelligence operations were conducted in the latter part of the 21st century, by the year 2000, a succession of computer worms, notably the Morris worm and the Y2K problem itself, had attracted the public's attention, as well as the attention of adversaries who were previously unaware of their vulnerability. Doors started slamming shut around the world as the United States lost access to previously "wide-open" systems. We responded, as America is accustomed to do, by throwing money at the problem. IO became synonymous with a mix of critical infrastructure protection and a mad dash to penetrate any and all computer systems without regard to cost-benefit analysis. We also failed to invest in Tasking,

Processing, Exploitation, and Dissemination (TPED), burdening our all-source analysts with increased volumes of captured information, while providing them with virtually no tools for making sense of that information.[14] Neither the U.S. intelligence community, nor the operational commanders ostensibly responsible for "requirements," actually produced any coherent requirements. IO was "collection-centric" and lacking in focus on definition of requirements, collection management, postprocessing, sense-making, or even actionable intelligence. The system was on auto-pilot, going over a cliff.

We went over the cliff on September 11, 2001 (9/11). Despite such books as *American Jihad* and *Bin Laden: The Man Who Declared War on America*,[15] despite a prior car bomb attack on the World Trade Center (and the capture of an entire apartment's documents that the Federal Bureau of Investigation (FBI) failed to translate), despite the FBI's timely capture of a key 9/11 participant with his laptop (which FBI lawyers would not allow to be examined), we failed to prevent 9/11. The only airplane that failed to hit its target was taken down by heroic U.S. citizens acting on public "intelligence" obtained by cell phone. This is a key observation: informed citizens acting on open source information can make a difference.

The events of 9/11 put the champions of open source information (OSIF) and open source intelligence (OSINT) over the top. Although the *status quo* bureaucrats and their legislative allies defeated virtually all of the intelligence reform recommendations put forward by genuine reformists, including the widows and orphans of 9/11,[16] proponents for transformative OSINT, aided by an open-minded USDI and Congressman Robert Simmons (R-CT-02), were able to leverage the tiny little box of recommendations on p. 413 of the 9/11 Commission Report (recommending an Open Source Agency coequal to and completely independent of the Central Intelligence Agency (CIA),[17] and related recommendations from two Defense Science Board reports, to achieve independent operating status within DoD.[18]

The "content" aspects of IO are now in the ascendancy. IO content can be thought of in two parts: Strategic Communication (the message) and OSINT (the reality). The first cannot be effective without the second. It is not possible to craft the right message, nor to deliver that message to the right person at the right time in the right

context, without first understanding "ground truth" at a substate level of granularity (tribes, villages, neighborhoods). OSINT is the horse seeing the path, strategic communication is the cart carrying the message. One must precede the other.

At the same time, it is not possible for DoD to be effective at either strategic communication or OSINT if each of the Combatant Commanders (COCOM) and each of the services is executing contracts willy-nilly for either outgoing messages or incoming reality, with a variety of contractors and a variety of systems and products that never come together in any one place nor in a fully interoperable relationship. Content needs standards as much as any system. It is especially important that USSTRATCOM, which has the IO message/reality mission, and USSOCOM, which has the Global War on Terror (GWOT) mission (and also the nation's finest operational OSINT capability),[19] form an "IO Axis" that each of the COCOMs and the services, as well as DoD intelligence agencies, can plug into. Expenditures on IO/OSINT (including man-machine foreign language translation) by the National Security Agency (NSA), the Defense Intelligence Agency (DIA), and the Intelligence and Security Command (INSCOM), to take three examples, must be managed by USDI or an operational field activity reporting to USDI in a manner such that we optimize what we spend and how we exploit what we capture or buy.[20]

Finally, there are two vital aspects of IO that USDI appears to be pursuing: DoD must serve a critical role as, first, the "hub" for interagency information-sharing within the U.S. Government and down to the state and local authorities; and second, as a bridging network across multinational multiagency boundaries, enabling more intimate and respectful information-sharing operations with coalition partners and NGOs than ever before, generally via the COCOMs and their JIOCs.

In summary, modern IO, the new IO, has three parts:

- Strategic Communication (the message),
- Open Source Intelligence (the reality), and
- Joint Information Operations Centers (the technology).[21]

With the foregoing discussion as preamble, the six IO-heavy mission areas will be reviewed in Chapter 2 with comments on the importance of DoD IO to the revitalization of national education and national research. Following a review of the mission areas, information challenges at each level of analysis (strategic, operational, tactical, and technical) will be examined in Chapter 3, as well as the strategic concepts for global IO. Chapter 4 sets forth the requirements statement for integrated IO. Chapter 5 contains conclusions and recommendations. The Appendix illustrates two analytic models for modern IO.

CHAPTER 2

THE IO-HEAVY MISSION AREAS

Peacekeeping Intelligence.

Peacekeeping Intelligence (PKI) is reactive, and must always be distinguished from Information Peacekeeping (IPK), which is proactive. PKI has been demeaned and ignored by United Nations (UN) leaders for decades. UN successes in the field, for example in the Congo in the 1960s, have occurred only when Force Commanders or selected national elements have chosen to ignore UN bureaucratic prejudices against the practice of sensible all-source military intelligence.[22]

In 2000, errors of the past were recognized, and a dramatic change in UN attitudes began to occur.[23] No longer a dirty word, "intelligence" increasingly was understood to be essential to the accomplishment of the UN mission at multiple levels.[24]

*Strategic***.** At the strategic level, the UN traditionally goes wrong in two ways: failing to act soon enough for lack of compelling early warning, and failing to provide the correct mandate for the peacekeeping or peace enforcement mission.[25] The mandate is the basis for both the timing and the composition of the operational force to be employed. Intelligence is now valued at this level.

Operational. At the operational level, the UN in the past has sent the wrong mix of forces, generally lacking organic intelligence capabilities spanning the full range from aerial imagery and unmanned aerial vehicles (UAV), to signals intelligence interception capabilities, to human intelligence and counterintelligence personnel, to qualified trusted translators. Intelligence is now impacting on this level.

Tactical. At the tactical level, the UN often has failed because the contributing nations' military elements are not trained, equipped, or organized for operating in a failed state environment, and such law enforcement elements as might be included in the UN force structure tend to be both illiterate and incapable of driving a vehicle, much less operating a computer.[26] Every Force Commander is now demanding organic capabilities.

Technical. At the technical level, the military forces assigned to the UN peacekeeping mission often will fail because their traditional intelligence collection equipment is unsuited for urban areas; for distribution down to the squad level; or for focusing on targets that do not "emit," wear uniforms, carry visible arms, or ride in conventional military vehicles with clear markings and known signatures. Force Commanders are buying hand-held video cameras and other devices out of their own personal funds and sharing knowledge about unconventional intelligence sources and methods, including open sources and methods.

In recognition of the urgent need for new and original concepts, doctrines, sources, tools, and methods for the conduct of PKI, the Swedish Supreme Commander has directed the establishment of a Peacekeeping Intelligence Course to be offered each March-April in Sweden.

Each of the IO initiatives being sponsored by USDI has considerable potential in support of PKI. Supporting PKI, and UN Force Commanders in the field, will reduce demands for unilateral U.S. force deployments, and also increase opportunities for transitions from hostilities to stabilization and reconstruction operations.

In concluding this section, we may note three areas where the UN and the United States have mutual interests and possibilities.

Maps. The single biggest deficiency in PKI is the almost total lack of 1:50,000 combat charts with elevation contour lines for the 90 percent of the world where instability is endemic.[27] In the Congo, for example, where Major General Patrick Cammaert is now the Force Commander, the National Geospatial Agency (NGA) has only seven out of the over 3,000 1:50,000 sheets needed for tactical military operations in that area. For under $1M, East View Cartographic, the private sector counterpart to NGA, can produce the 191 most critical map sheets needed for peacekeeping operations in the Congo. There is a need for a robust USDI program to accelerate the commercial production of tactical military maps needed by the UN and also needed by any U.S. forces engaged in follow-on stabilization and reconstruction missions. If it can be done in the private sector, it should not be done by NGA, which has more urgent and sensitive demands on its capabilities.

UN Centers. Prior to departing his assignment as Military Advisor to the Secretary General, Major General Cammaert cited a need for Joint Military Analysis Centers (JMAC) in each conflicted region. The first is being established in Africa, where it is widely understood that a regional approach to intelligence is necessary. Single country intelligence centers and intelligence campaign plans are ineffective. When attempting to interdict smuggled small arms, mercenaries, unauthorized Private Military Corporations (PMCs),[28] blood diamonds, trade in women and children, or illegal funds transfers, only a regional approach stands any chance of being effective. There is real potential in the USDI interest in creating replicable JIOCs, in that a planned overlay and planned interoperability between U.S. JIOC and UN JMAC could have very positive outcomes in support of the four salient regional objectives—Diplomatic, Information, Military, and Economic—which I incorporate in the acronym DIME.

*Open Source Intelligence (OSINT)***.** While the UN has now accepted the importance of intelligence or decision support, the member nations are not about to give it substantial classified intelligence support, and the reality is that most classified intelligence capabilities are relatively useless in failed state environments. The one area where the UN and DoD have absolute common cause is that of OSINT. To paraphrase Hugo Smith, as he put it so well in 1994, UN intelligence, by the very nature of UN operations, is best when it is overt, using methods that do not compromise the integrity or impartiality of the UN, when the information can be shared and become widely known.[29] There is every reason for DoD to establish information-sharing agreements with the UN for each of the complex emergencies where military personnel are operating, and with other NGOs as appropriate.[30] Indeed, in the OSINT arena, one can easily perceive the potential value of UN leadership in OSINT, with DoD subsidizing a mix of NGO and Google-like private sector initiatives.

Information Peacekeeping.

The concept of "information peacekeeping" or IPK emerged in the late 1980s when the author first tried to get a grip on global coverage and realized that no one nation, hence no one intelligence agency, could succeed on its own, and began devising concepts for an

information continuum, burden-sharing, and "virtual (distributed) intelligence communities that fully engaged the private sector.[31]

In 1997, based on my conversations within the United States Institute of Peace (USIP) and my work on an invited paper entitled "Virtual Intelligence: Conflict Avoidance and Resolution Through Information Peacekeeping," the concept emerged in full form at the Virtual Diplomacy conference of April 1-2, 1997.[32] In the development of my ideas, a negative evolution—the growing gap between elites with power and experts with knowledge—was offset by the slow but steady emergence of what is today called "collective intelligence" or "wisdom of the crowds."[33]

The paper emphasized that the core competency for diplomats was the harnessing of distributed unclassified knowledge, or "tools for truth," in order to discover, discriminate, distill, and disseminate knowledge helpful to both protecting national security and nurturing national competitiveness.[34] The following general principles of information peacekeeping are discussed in the closing section of the paper, which was published 8 years ago, and remain relevant today to the design and implementation of modern IO.

- Information peacekeeping is the ultimate global presence.
- Information peacekeeping is the *first* policy option—both to ensure that the policymaker has a full knowledge of the situation, and to impact constructively on those we seek to influence.
- We need to develop an information peacekeeping "order of battle," with related tables of organization and equipment—most of which 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 require the virtual constant integration of law enforcement, military, and civilian agencies as well as all elements of national intelligence into a larger secure global information architecture.

- Information is the ultimate *countervailing force* against the emerging threats, and the most cost-effective means of devising diplomatic and other responses intended to avoid or resolve conflicts.
- At least 80 percent of the information the policymaker needs in order to conduct information peacekeeping operations is not controlled by the government: "Knowing who knows" and the creation of management, technical, security, and procurement architectures that permit harnessing the distributed intelligence of the entire world (not just U.S. citizens with clearances), are the emerging new sources of national power.
- Because the policymaker is inundated with contradictory information lacking systematic evaluation, a critical priority must be the transfer of the proven methods of classified intelligence analysis to the world of unclassified information.
- Unclassified information is critical to converting policymakers' minds and winning public hearts. The policymaker *can* succeed without classified information but he or she *cannot* succeed without a mastery of unclassified information.
- Multichannel delivery of "truth" is the SIOP[35] 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,[36] and from dimension to dimension.[37] The greatest challenge for the policymaker will be to manage a national intelligence and information-sharing architecture that can rapidly identify the information center of gravity, prepare the information "battlefield," and deliver the appropriate (non-lethal) information "munitions" to carry the day.

IO is ultimately about using information as a substitute for conflict and as a means of creating wealth that stabilizes the now impoverished regions of the world.

Early Warning.

We do not lack for sources and methods relevant to Early Warning, although we could certainly do vastly better simply by attending to all sources in all languages all the time. What we lack is imagination on the part of analysts, who are largely young, white, bland, and distanced from foreigners; and focused attention on the part of policymakers. Kristan Wheaton, one of America's most talented defense attaches at the time he wrote the book, *The Warning Solution: Intelligent Analysis in the Age of Information Overload*, makes three important points:[38]

- **Policymaker Overload**. Referring specifically to Kosovo, he points out that the U.S. European Command all-source analysts had all the warning they needed, but could not "break through" to the bosses because, at the time, Kosovo was a $1 billion problem, and the policymakers, including the Supreme Allied Commander, were preoccupied with $50 billion dollar problems.
- **Iconoclasts Need Not Apply**. Overloaded policymakers, and the all-source managers of analysts who serve them, do not like to be made uncomfortable by iconoclasts and mavericks. Not only does "the system" not search for such individuals, it actively shuts them out.
- **History and Culture Ignored**. In specific relation to the Kosovo campaign and the early warning that was both achieved and not achieved, he stresses that it is human understanding of historical and cultural facts and biases, not current intelligence captured through technical means, that really puts the meat into Early Warning.

We do receive some Early Warning *from* analysts, and we can increase that by a factor of 1,000X if we get a grip on what the Swedes call M4 IS: multinational, multiagency, multidisciplinary, multidomain information-sharing. However, regardless of how much substantive Early Warning we have, our biggest problem remains a lack of Early Attention *by* policymakers. In addition to

the ideas put forth in Kristan Wheaton's work, we have a book by Thomas Davenport and John Beck titled *The Attention Economy: Understanding the New Currency of Business*, which is dedicated to the topic of organizational "attention deficit disorders."[39] They also offer useful suggestions. First, they recommend that resources be allocated, and management attention be structured, along the following lines:

Global coverage for AWARENESS. In contrast to the current obsession with terrorism, which is no higher than number five or six on most professional threat lists[40] and which has joined the "hard targets" of the past as the focus of loosely-coordinated effort among the classified agencies, these authors recommend a global spider web, very lightly spun, to capture those weak signals, many of which will pertain to topics (for example, the emergence of bird flu in China) that are not normally sought by classified means. The recommendation of these authors tallies precisely with a report done for George Tenet, then Director of Central Intelligence, titled *The Challenge of Global Coverage*. Delivered in July 1997, this report recommended that $1.5 billion a year be spent, comprising $10 million for each of 150 combined "low priority" countries in the Third World addressing specified nonconventional targets, including disease, poverty, water scarcity, etc.. The report was promptly filed and forgotten. Just as in the old DoD, where a Chairman of the Joint Chiefs of Staff was quoted as saying, "Real men don't do Operations Other Than War," the leadership of the U.S. intelligence community remains convinced that they are in the business of generating secrets for the President, and there is but lip service given to meeting the needs of all federal agencies at all levels, with no appreciation at all for the value of public intelligence.[41] The good news for all of us, as validated by such distinguished authors and practitioners as Dr. Michael Herman of Oxford,[42] is that global coverage can be largely accomplished through free and low-cost monitoring of open sources of information in all languages, all the time. Somebody has to do it, and that somebody is probably the private sector, under mandate from DoD, and with virtual global collaboration from coalition militaries in every country.

Surge local focus for ATTENTION. Classified assets simply do not surge. Classified imagery satellites are optimized for hard targets and do not do well against jungle canopy or caves in mountains. Signals

capabilities are terribly ineffective against Third World languages and fast-changing signatures. Clandestine assets tend to be clustered in the capital cities and focused on the cocktail party circuit. They also do not transfer well—in one case, two clandestine case officers sent to Somalia without language skills literally became unhinged, according to an extensive investigation by *The Washington Post*. In contrast, private sector capabilities, with all necessary language and local knowledge qualifications, focused on open sources can surge very ably.[43] Commercial imagery on demand within 2 days, with 2-day repeat cycles, and 1-meter resolution? Broadcast monitoring, local area gray literature collection, mosque sermon monitoring, a photograph of an arms dealer's front door taken with a cell phone camera, boots on the ground for verifying whether the new uranium mine really exists? No problem. Not only no problem, but available at a fraction of the cost of a classified asset. All you need is a decent budget and a mind-set acknowledging that legal and ethical open sources of information just might be your best option. It bears mention that open sources can be discreet—commercial enterprises and private investigators routinely sign and enforce nondisclosure agreements with severe penalties for infractions.

Domestic political focus for ACTION. Early Warning that is classified can be safely ignored by officials—there are rarely any political consequences for pretending that certain intelligence does not exist. In contrast, well-structured, well-documented public intelligence, ideally with strong visuals, can have a "CNN effect" on policymakers, forcing them to at least consider some form of action. Commercial or open source information is also shareable easily with Congress, close allies, near-at-hand coalition partners, and even distrustful countries and activist organizations.

Davenport and Beck go on to cite relevance, community, engagement, and convenience as the four key factors in attracting and holding the attention of individuals and to specify four "attention tracks" that each analyst or policymaker must manage: focusing one's own attention; attracting the right kind of attention to oneself; directing the attention of those under one's oversight; and maintaining the attention of one's customers and clients.

Decisionmaker inattention is not unique to government. The most acute observer of the global business intelligence scene is an

Israeli, Ben Gilad, who tells us:

> One of the facts that amazed me the most over the past 8 years while helping American and European firms improve their ability to read their markets, was how insulated top executives were from competitive reality. This is because they secure their competitive intelligence (market signals regarding change) at best through a close circle of "trusted" personal sources, or at worst through those one-page news summary clippings. *Top managers' information is invariably either biased, subjective, filtered, or late.*[44]

Moreover, problems of poor performance characterize America's scientific and technical (S&T) communities. Bradford Ashton and Richard Klavans, the two top practitioners in America in the field of predictive analysis for S&T, state: "The practice of applying intelligence principles to science and technology (S&T) in business is a new field . . . . Unfortunately, at this time, information on the practice of [competitive technical analysis] in business is diffuse and fragmented."[45]

While there are some bright spots, such as the Academy of Competitive Intelligence organized by Jan Herring, a former National Intelligence Officer for Science & Technology[46] in partnership with Ben Gilad and Leonard Fuld, and there are a few exceptional practitioners here and there,[47] by and large business intelligence is in the basement—one- and two-person shops cutting and pasting and without the budget or the tools or the mindset to do Early Warning or Predictive Analysis.

Stabilization and Reconstruction Operations.

Congress had to legislate the capabilities for Special Operations and Low-Intensity Conflict, as well as the requirement for jointness (Goldwater-Nichols Act). Today DoD is more mature and more open-minded. It is DoD that has taken the lead in defining, through the Defense Science Board, a need to move smoothly into the business of Stabilization and Reconstruction.[48] It is DoD that sees clearly the need for joint interagency collaboration and information-sharing centers. It is DoD—not the mandarins of classified intelligence—that sees the value of close and open collaboration with NGOs using the

civil affairs model for multilateral liaison, rather than the intelligence model of compartmented bilateral liaison. DoD has, in short, come of age.

We are moving, in simplistic terms, toward four "forces after next" to address the four emerging types of conflict:[49]

- Big War/Information Operations (USSTRATCOM)
- Small War/Global War on Terror (USSOCOM)
- PeaceWar (Not Yet Assigned)
- Homeland Defense (U.S. Northern Command [USNORTHCOM]).

By way of introduction to Stabilization and Reconstruction (S&R) operations, we would make two observations: first, that there are growing calls for a unified national security budget, in which diplomatic, military, and law enforcement investments and capabilities are orchestrated within a coherent strategy rather than in their current stovepiped isolation;[50] and, second, that Singapore is leading the way in focusing its Ministry of Defence on all threats, whether man-made or not. The appearance of Severe Acute Respiratory Symptoms (SARS) was a wake-up call for them. Such an "attack" could wipe out their population in a matter of weeks. "Defense" today must be global, integrated, and prepared for all threats, both those that involve a heavy metal military, and those that require operations other than war (OOTW), including medical prevention, interception, and recovery.[51]

In my 2002 work, *The New Craft Of Intelligence: Personal, Public, and Political*, I devoted five chapters to unconventional threats—global conditions including poverty and mass migrations that spawn terrorism; plagues, toxic bombs, resource wars, and water shortages; and global genocide—and to these we would today add support for numerous dictators[52] and various immoral manifestations of capitalism, both of which undermine any public diplomacy or strategic communication message we might wish to deliver.

For the sake of emphasizing the importance of the S&R mission, which has yet to be assigned, and which could reasonably be either an addition to USSOCOM or a new interagency Combatant Commander,

let us briefly review the "state of the world" as various troubled nations impact on U.S. national security in the form of increased threats from illegal immigration, energy supply interruptions, water shortages, the spread of pandemic disease, crime, terrorism, etc.:[53]

- Complex Emergencies: 32 countries
- Dictators Supported: 44 countries
- Refugees/Displaced: 66 countries
- Starvation: 33 countries
- Plagues: 59 countries
- Ethnic Conflict: 18 countries
- Child Soldiers: 41 countries
- Censorship: 62 countries
- Water Scarcity: widespread
- Resource Wars: widespread.

DoD's new-found focus on S&R is very wise. Not only are there not enough guns on the planet to enforce security[54] (peace is security without force; security is enforced peace),[55] but it clearly has been established by numerous authorities that the combination of legitimacy[56] and localized wealth creation is the sine qua non for stabilizing and nurturing large populations. Corruption and censorship undermine wealth creation. Neither benign dictatorships nor a dramatic increase in foreign aid will do it. We need to nurture the three billion new capitalists of China and India, not fear them.[57] Information, not foreign assistance, is the key to this mission.

Homeland Defense and Civil Support.

DoD has recently published a clear mandate on this topic in a document titled *Homeland Defense and Civil Support*.[58] It espouses a defense in depth. As stated on the first page:

> This active layered defense is global, seamlessly integrating U.S. capabilities in the forward regions of the world, the global commons of space and cyberspace, in the geographic approaches to U.S. territory, and within the United States.

We would add two observations: first, that the single "constant" between DoD and the Department of Homeland Security (DHS) is information and intelligence; and, second, that in this age of improvised terrorism where sleepers already in the United States use commercial vehicles and local supplies to attack homeland targets, the only thing that can be intercepted and acted upon is information.

The capabilties for Homeland Defense and Civil Support as particularly emphasized in the DoD strategy document (pp. 3 and 4) are as follows:

- Intelligence, Surveillance, and Reconnaissance
- Information-Sharing
- Interagency and Intergovernmental Coordination
- Joint Operations (for Homeland Defense).

The first three of the four capabilities are focused exclusively on information and intelligence, while the fourth demands the fullest possible implementation of common interoperable command and control, communications, and computing (C4I) systems. Since DHS and its constituencies cannot afford the high-end systems that DoD has been funding for itself, and DoD cannot afford to pay for 50 to 5,000 C4I nodes across America, there is only one option: an open source software solution that allows everyone to tie in to a new Open Source Information System-External (OSIS-X),[59] and the melding of OSIS-X into an Application-Oriented Network (AON)[60] that permits the sharing of secret information on a by-name basis regardless of nationality 24/7.[61]

There is a subtlety involved in all this that requires strong scrutiny by both DoD and DHS information and intelligence managers. While DoD can and should be responsible for global monitoring in support of defense missions, we must be accutely conscious of the possibility (in my opinion) that 50 percent of the "dots" relevant to preventing the next 9/11 will be "bottom-up" dots collected at the county level by direct observation from citizens, public employees, and law enforcement professionals. Today those dots have no place to go. Although congressional hearings have been held and will be held again on the need for a national domestic intelligence network,[62] DoD

should consider a pilot project with the U.S. Northern Command (USNORTHCOM) and a few key states (e.g., New York, Texas, Virginia) in which DoD's man-machine foreign language processing capabilities are made available to all 911 operators, at the same time that a new number, 119, is established as a pathway for citizens to report via locationally-aware voice, image, or electronic message, any suspicious individuals, packages, or activities.

More specifically, it is imperative that DoD expand its vision for IO to include a recommendation to the President that DHS receive a matching investment of $1.5B a year for 50 state intelligence centers and networks, each funded at $30M per year at final operational capability. The National Guard is uniquely qualified to man those centers, since it can hold both military commissions with access to national foreign intelligence, and state law enforcement commissions with access to citizen information under strict privacy protection. Guardsmen are, not, however, qualified to design or build these centers. A special DoD-DHS task force is recommended.[63]

Homeland defense suffers from one major handicap that must be overcome, the same handicap that prevented the FBI from being effective in the months leading up to 9/11. Lawyers, including especially lawyers at USNORTHCOM, are both uninformed and timid when it comes to a determination of what can and cannot be collected and exploited when using open sources of information about U.S. citizens or foreigners within the borders of the United States.[64] It would be most helpful if DoD established, in partnership with the Department of Justice, a legal working group with a 24/7 Help Desk able to protect the Combatant Commanders, the National Guard, and others, from their own lawyers whose timidity-based ignorance leads them to say "no" when they actually have no idea what the law allows.

National Education and National Research.

The failure of education in the United States, in which U.S. students consistently are falling behind Indian and Chinese students—as well as Nordic and many other nationalities—has been the subject of many books and commentaries and will not be examined in detail here. However, it is vital to understand that one cannot have smart

spies in the context of a dumb nation, nor can one have effective OSINT or effective strategic communication (and public diplomacy) if these are perched on a hollow shell.

In addition to failing at science and technology, with a majority of our engineering and computer science graduate students now hailing from outside the United States rather than from within our own citizen base, we have the problem of insularity. Both David Boren (former Chairman of the Senate Select Committee for Intelligence, today the President of the University of Oklahoma) and David Gergen (former Senior Editor of *U.S. News & World Report* and presidential advisor) have called for the "internationalization of education."[65] Both fear that our children—and their parents—are so intellectually and emotionally isolated from overseas realities as to foster an attitude of neglect among our political leaders.

With the collapse of education comes the collapse of research and then development across all S&T domains. Lou Dobbs on CNN has focused on the out-sourcing of jobs from America. Now Thomas Friedman of the *New York Times* points out in emphatic terms that America is losing basic research and development work, the heart and soul of modern productivity and wealth creation, to China and India.[66]

It is all interconnected. My view is clear-cut: IO and national intelligence writ large (i.e., truly national, embracing all elements of society, not only the spies and purveyors of secrecy) are potentially the "lifeboat" for rescuing America from its intellectual and moral decline.

Unlike the Vietnam era, when DoD was asked to help create the Great Society by absorbing into the Army Category IV individuals who were "brain challenged," we are today in a completely different situation. DoD has an opportunity to recruit and nurture the best and the brightest, to achieve universal coverage, 24/7, in all languages, and to cycle the resulting "ground truth" back into society and particularly back into the classroom, as well as across the national S&T laboratories.

In combination, legal and ethical Strategic Communication, OSINT, and joint interagency information-sharing entities can revitalize the nation. We must "think big" and "dare to want it all."

Not Covered by This Monograph.

This monograph does not cover the dramatic exponential changes that are occurring in the information technology arena writ large, namely, the changes characteristic of information about and within genetics, robotics, nano-technology, and the related fields of cognitive science and informatics. We agree with those who believe that advances in information technology could produce revolutionary wealth and revolutionary solutions to the problems that plague the world, including poverty, pestilence, pollution, and the vanishing of our most precious resource, water. However, we also believe that the humanities are behind the sciences, and that Henry Kissinger is correct in saying that the sources and methods of governance are not keeping pace with the scale and speed of the challenges to governance.[67] It is my view that IO, if carried out by DoD in the enlightened manner that is potentially possible, has the possibility of revolutionizing governance by revolutionizing what government can know, how it knows it, how it decides, and how it communicates both its decision and supporting information. Modern IO is the first step toward revolutionary wealth.[68]

CHAPTER 3

INFORMATION CHALLENGES

The Strategic Problem.

At the strategic level and directly related to a half-century of focus on a handful of hard targets considered to be military threats, the United States finds itself with a military optimized for force-on-force confrontations between nation-states and a national intelligence community optimized for stealing secrets through technical means, with an extremely limited range of focus and almost no flexibility. The bulk of the money for intelligence is invested in technical collection rather than in Tasking, Processing, Exploitation, and Dissemination (TPED).[69] Of intelligence funding, 99 percent is focused on secret collection rather than open source information acquisition and exploitation. Emerging threats and nonstate actors are best understood through realization of Dr. Cambone's vision of universal coverage, 24/7, in all languages, using open sources of information. At the same time, DoD lacks adequate personnel with language skills relevant to most of the complex emergencies and conflict zones where U.S. forces are engaged.

Here following are pointed words taken from recent official pronouncements of the U.S. Government on the strategic problem under discussion:

> Much of the needed information and knowledge can be found in unclassified sources, [but] the pursuit, exploration, and exploitation of open sources have taken a back seat to learning secrets. While we in no way denigrate the importance of the latter, we ask the [Secretary of Defense] to instruct [the Defense Open Source Council] to establish a vital and active effort focused on using open sources to provide information on cultures, infrastructure, genealogy, religions, economics, politics, and the like in regions, areas, and states deemed ripe and important.[70]

> DoD does not have an effective language oversight program. There is no systematic requirements determination process. There is no comprehenisve and accurate database of DoD personnel with language skills. . . . What we [must be] concerned with is . . . anticipating tomorrow's requirements.[71]

> [T]he need for exploiting open source material is greater now than ever before . . . since the spread of information technology is immune to many traditional clandestine methods of intelligence collection . . . open source materials may provide the critical and perhaps the only window into activities that threaten the United States.[72]

The Operational Problem.

At the operational level, interagency collaboration within the U.S. Government, federal-state-county collaboration among the three levels of homeland governance, and multinational interagency collaboration within any given regional theater of operations are severely constrained, almost to the point of complete ineffectiveness. The cause is decades of investment in unilateral classified communication systems to which others—including elements of the federal government not traditionally engaged in national security affairs and U.S. law enforcement at the state and local levels—cannot be granted access. The problem is exacerbated during the transitions to and from hostilities, on behalf of which the Defense Science Board has determined that information-sharing with NGOs is absolutely essential to both campaign planning for military operations and the execution of post-hostilities S&R operations. The problems evident in our own homeland security information environment are compounded dramatically when we are seeking to access and exploit foreign information.

> Today there is no single agency or computer network that integrates all [national] security information [worldwide] . . . instead, most of the information exists in disparate databases scattered among federal, state, and local entities. In many cases, these computer systems cannot share information—either "horizontally" (across the same level of government) or "vertically" (between federal, state, and local governments). Databases used for law enforcement, immigration, intelligence, and public health surveillance have not been connected in ways that allow us to recognize information gaps or redundancies.[73]

> The USG cannot meet its own obligations to the American people to prevent the entry of terrorists without a major effort to collaborate with other governments. We should do more to exchange terrorist informatin with trusted allies. . . .[74]

The Tactical Problem.

At the tactical level, two problems persist, one from the past and one newly recognized. The continuing problem is associated with the disconnect between classified national systems that cannot see under bridges, within neighborhoods, and into hearts and minds; and the distinct but related problem of delivering useful fused intelligence to the front lines—to the those fighting to achieve objectives in the last mile. The newly recognized problem, dealing with the proliferation of coalition allies, NGOs, private military contractors (PMC), religious organizations, and increasingly self-organized citizens groups, is that of establishing effective means both of sharing unclassified information when it makes sense to do so, and of establishing a shared view of the battlefield, be it diplomatic, informational, military, or economic.

The other tactical problem is within the homeland security environment. DoD is totally correct to focus on defense in depth, but right now the troops on the front line—our citizens, local police, paramedics, and firefighters—are completely outside of the C4I "loop." DHS has labored heroically to address this problem, and there are close to 30 different C4I systems reaching various state and local authorities in generally convoluted and difficult-to-use ways. However, the reality is that DoD needs to suggest to the President—the only person who can make this decision—that the time has come for America to have an end-to-end C4I system that goes from schoolhouse to White House—every agency, every office, every state, every county, every university, every business, every labor union, every religious parish—needs to be able to plug in to a national intelligence and information-sharing architecture, with the state intelligence centers and networks as the "hubs" for state-based information-sharing. Roughly 90 percent of what everyone knows is not secret, so it makes sense to focus this new tactical system on unclassified commoditized elements, rather than trying to force fit an unaffordable Sensitive Compartmented Information (SCI) architecture to a role it simply cannot fulfill.

The Technical Problem.

Available information in 33+ languages and at least 12 dialects of Arabic has proliferated geometrically.[75] Not only has print media information grown beyond all bounds, but African, Arabian, and Asian radio and television have done so as well. They are often the only sources available to illiterate individuals comprising a breeding ground for terrorists and criminals. Our national systems—both technical and human—are unable to muster the effort to acquire, translate, and analyze all relevant open information. At the same time, much of what we know is buried in electronic mail and personal hard drives that are not normally indexed for search and retrieval by any enterprise-wide system, much less a network. Tactically, there is a need for a leap ahead in both Personal Digital Assistant (PDA) technology, and in the exploitation of globally distributed multimedia and multilingual information for specific localized needs.

STRATEGIC CONCEPT FOR GLOBAL IO (M4 IS)[76]

Appreciating the Magnitude of the Challenge.

The global information explosion and its logarithmic increase cannot be understated. Figure 2 illustrates where information quantities are headed. Information has doubled over these past 2 years, so we are now looking at 100 billion gigabytes or 100 exabytes, roughly equivalent to 2 trillion four-door filing cabinets of hard-copy documents.[77] Within this complex multimedia and multilingual environment, the noise to signal ratio will get tougher, and so also will the early warning, anomaly detection, and pattern recognition challenges.

This is just the *digital* information—when one adds unpublished local or expert knowledge, locally-available hard copy or "gray literature," and geospatial information as well as television and audio programming not available through the Internet, the awesome magnitude of this challenge becomes apparent.

The critical ingredient in making sense of all this information in near real-time is a scalable database architecture that is capable of real-time content-based routing; high-speed, continuous indexing;

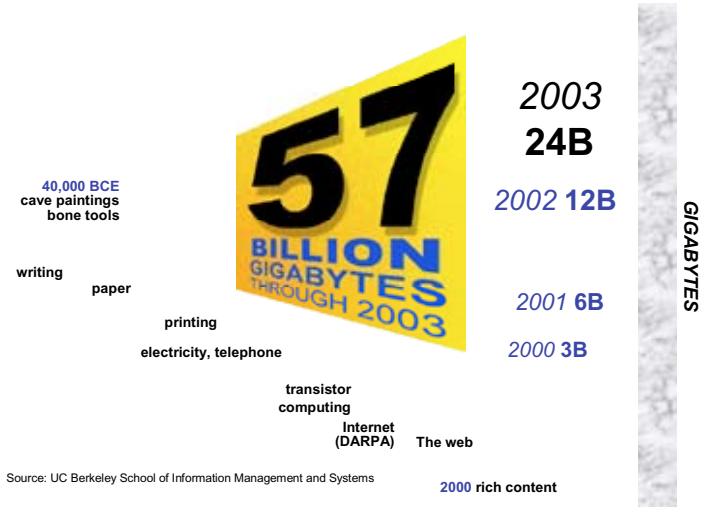


Figure 2. The Growth of the Global Information Challenge.

and rapid search-and-retrieval across all relevant databases both public and private.

Linking Strategic Communication and Special Operations.

From my perspective, the IO mission of USSTRACOM and the GWOT mission of SOCOM comprise the two ends of an axis along which all other Combatant Commanders; defense agencies; and federal, state, and local information operations—especially public diplomacy by the Department of State and commercial risk monitoring by the Departments of Commerce and Treasury—can "plug in." The STRATCOM investments planned for global IO and the SOCOM investments planned for enhanced information technology applications and open source intelligence can and should be integrated by USDI using a commercial "virtual back office" for unclassified DoD information.[78]

There are other major contributors, notably elements of the UN engaged in peace enforcement operations and in S&R missions, and international law enforcement activities focused on capturing and containing terrorists, arms proliferators, and smugglers. This

strategy is consistent with Office of Management and Budget (OMB) interest in considering the maximum possible use of commercial providers of open source intelligence collection and processing in behalf of defense and homeland security.[79]

Within the U.S. Government, the search for "common solutions" by OMB could be substantially enhanced if DoD were to fully integrate experts on the U.S. Federal Enterprise Architecture (FEA), the Data Reference Model (DRM), and the National Information Exchange Model (NIEM) into its planning and oversight of contracts related to interagency collaboration and information-sharing centers.[80]

The Department of State deserves special mention. Although historically it has been the primary collector, processor, translator, interpreter, and disseminator of foreign language information relevant to U.S. national security and foreign policy, over time it has chosen to become an end-user of intelligence and to abdicate its role as the nation's primary overt collector and evaluator of foreign information. This monograph respects State's preferences, but advocates a partnership between State and DoD in which DoD provides State with 10 nonreimbursable personnel positions with which to create an Office of Informaton Sharing responsible for negotiating information-sharing treaties with nations and information-sharing agreements with organizations, including NGOs, universities, and other private sector parties. We also recommend that State, along with DHS, be treated as "first among equals" as clients for the DoD IO system.

The U.S. Departments of Commerce, Treasury, and Transportation, as well as the Department of the Interior, also require special mention. Both Osama bin Laden and China understand that 21st-century warfare centers around economic advantage, not military advantage. Both are focused—the one for destructive reasons, the other for constructive reasons—on economic, trade, financial, and energy networks. It is not possible to protect U.S. national security nor to nurture U.S. national competitiveness without the application of the most advanced defense information and intelligence concepts possible to commercial, economic, treasury, transportation, agriculture, and health matters. It is all connected.

STRATCOM-SOCOM represent the first tier of connectivity.

DHS and NORTHCOM, followed by the regional COCOMs, are the second tier of connectivity. The rest of the government is in the third tier, while coalition governments and NGOs are in the fourth.

Creating the Open Source Information System-External (OSIS-X).

Figure 3 illustrates our understanding of the four quadrants of information that every COCOM and defense agency must be able to gain access to in order to plan and carry out their missions. Huge investments have been made in the two secret quadrants, but virtually no money at all has been spent on the two unclassified quadrants.

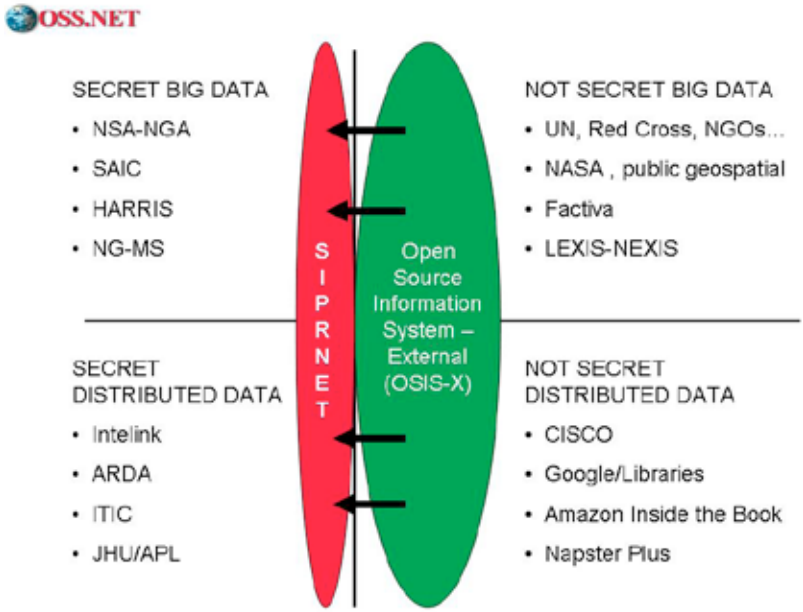


Figure 3. Open Source Information System-External.

DoD should deliberately fund OSIS-X as a commercial venture, taking care to migrate key personnel and standards from Intelink and OSIS in order to create a universal global network that can not only receive and make sense of all unclassified information in all languages and all mediums, but can also be paid for—in cash and in kind—by all governments, corporations, and transnational organizations that choose to participate.

The cost of global information to the government would be sharply reduced, in part by eliminating the need for multiple subscriptions to expensive commercial subscription and aggregation services[81] that have been overtaken by direct source access at lower cost via the Internet, and in part by creating a global network that facilitates the harnessing of distributed global intelligence that easily can be routed to the high side of government systems. This network should provide for the exploitation of leap-ahead commercial technology and new forms of security that will increase what can be shared and with whom under appropriate dissemination controls with workable audit trails.

Generic Information Collaboration Center.

The Joint Interagency Collaboration Center (JICC) initiative at SOCOM (see Figure 4) should become a replicable generic capability.

Such a capability could be migrated quickly from its first implementation at SOCOM, to STRATCOM and the Multinational Force in Iraq (MNF-I), then to other theaters (especially NORTHCOM for the homeland security implementation), thereafter to each state (creating generic statewide Community Intelligence Centers),[82] and then outwards to the varied NGO agencies that have important global databases and subject-matter expertise relevant to targets of mutual interest, including failed states.[83]

Creating Regional Multinational Centers and Networks.

OSIS-X could offer free uploading to all regional COCOMs and their coalition allies so that the information can be indexed, secured, and easily harvested to the high side by USDI's chosen integrator. The generic ICC should be migrated to regional multinational information-sharing centers that could eventually become multinational all-source intelligence and operations centers (see Figure 5) where coalition militaries can compile unclassified information from across their respective countries, while allowing a multinational team led by the United States to process and make sense of this information for regional early warning and action purposes.

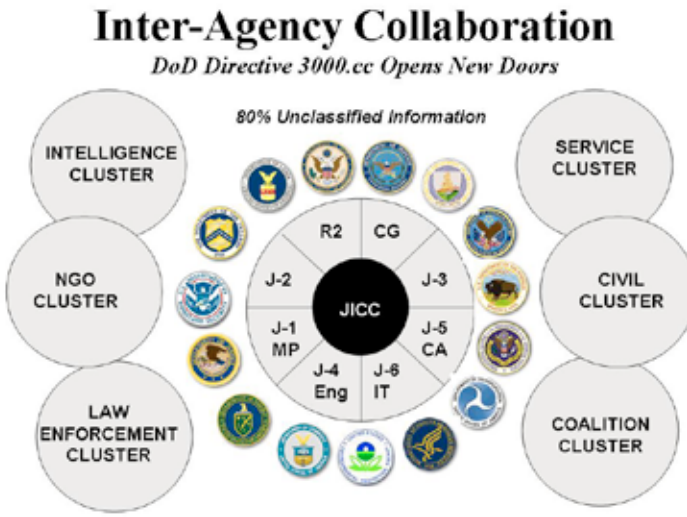


Figure 4. Providing a Generic Information Sharing Solution.

It will be important, if we are to honor NGO concerns about transparency and propriety, to keep the core regional information center "pure" by dealing only with open sources of information that can be shared with NGOs. However, the depiction in Figure 5 deliberately reflects a future evolution of such centers (or mirror centers at another location) into all-source collection management and processing facilities.

Global S&R Operations.

DARPA STRONG ANGEL[84] open source software appears to be relevant, in conjunction with INTER-4 tactical computers[85] sanitized for general use, to rapidly establishing both theater-wide and tactical information-sharing and collaboration networks. These networks would employ shared low-cost information analytics and decision-support features. Both NGO and the DHS constituencies (state and local governments) share a common problem: lack of funding for high-end communications and computing systems. The solution is to extend STRONG ANGEL to the point where it can be easily adopted by anyone as a basic desktop and/or hand-held toolkit. It should be possible for NGOs and for state and local governments to

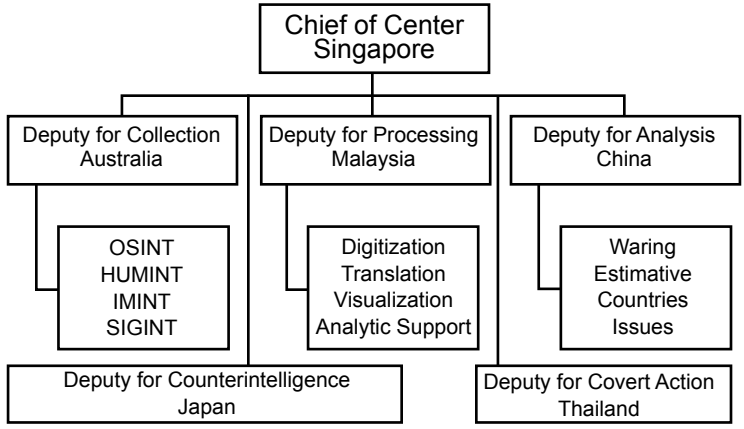


Figure 5. Concept for Harnessing Coalition Information.

contribute information to the DoD system at no cost to themselves, and for them to draw relevant information approved for release at no cost to themselves. Enabling this participation will substantially increase the amount of relevant unclassified information available to all DoD elements, while also enabling collaborative online work and information-sharing in near real time across all mission areas. This will also enable coalition partners who are not part of the North Atlantic Treaty Organization (NATO) and who cannot afford unilateral top secret systems to have a viable multinational, multiagency information-sharing toolkit available to them.

This is all the more true because the existing DoD Global Information Architecture (GIG) is both out of date and unaffordable by anyone else.[86] The high-end proprietary Information Technology (IT) solutions are not only too expensive, but also pathologically noninteroperable. Open source software and open (electromagnetic) spectrum are, along with open source information, the heart of 21st century IO. This wealth of knowledge can be mined by DoD if it makes open source software a viable option.

Harnessing the Seven Other Tribes.

Within each nation-state, the national government, the military, and the national law enforcement community represent just a

fraction of the local knowledge and the direct access to varied open sources of multilingual and multimedia information. The seven other "tribes" include the business sector, the academic community, the NGOs, the local or regional news media, and self-organized citizen groups, labor unions, and religious congregations. Our concept of operations provides for the facilitation of web-based voluntary but also *accredited and authenticated* participation by any and all elements whose employees will be afforded anonymous access across the system, with the entire process taking place generally through and with the encouragement of their governments. The creation of such networks within each nation-state, and within each region, actually facilitates strategic communication in that the same network used to receive open source information can also be used to broadcast, in a carefully measured manner, specific messages to specific groups.

It is important to stress that classified information is a small fraction of the relevant information needed for strategic communication, peacekeeping intelligence, information peacekeeping early warning, and S&R. The vast majority of the information needed by DoD is unclassified, generally not online nor subject to deep web data mining, generally not in English, and generally not readily identifiable unless a witting and willing volunteer from the owning organization "offers it up." Roughly 90 percent of the information we need is unclassified and available only from organizations that will not share that information with secret agencies. Civil affairs is the model to use.

Sense-Making.

The U.S. Government has some pockets of excellence in sense-making, but, in general, most of the government, including DoD, is still in the industrial era of paper reports and isolated human analysts trying to "connect the dots" without adequate toolkits. DoD needs a Strategic Decision-Support Center such as has been proposed by Captain Scott Philpott, USN, one of the original architects of the USSOCOM "pit." Such a Center must bring together in one place the following elements:

- OSINT super-searchers with global access;
- Classified super-searchers with full access to all raw secrets;

- Brainstorming network with both in-house and distributed experts;
- Geospatially and time/date-based visualization; and,
- Modeling and simulation using rapid response incremental approaches.

Putting the I Back Into Diplomatic, Information, Military, and Economic (DIME).

DoD needs to create or contract for a global open source acquisition, analytics, and technical information-sharing environment. It must be able to increase by an order of magnitude, and then a double order of magnitude, the near-real-time multilingual and multimedia information that can be delivered to DoD elements. It would be used to support operational planning, acquisition and logistics management, and all-source intelligence targeting, evaluation, and integrated production. This capability must merge global acquisition, translation, statistical analysis, analytic services (including historical and cultural analysis), and tailored dissemination in near-real-time. Such a capability will dramatically reinforce DoS public diplomacy, DoD strategic communication, and other missions, while being directly transferable to DHS. For example, the man-machine foreign language network can be used to reinforce all 911 Emergency Responder networks now lacking in foreign language capabilities.

The I, or Information, cannot be put back into DIME from the high side or secret side of the U.S. intelligence and information environment. It can be restored only from the unclassified side, the side that is open to both receiving information from external parties, and sharing information with those same parties. DoD, using the overt civil affairs model for liaison rather than the secret intelligence model for bilateral covert liaison, is the only element of the government capable of putting the I back into DIME.

Google, in the private sector, may offer a solution. Google is the only truly affordable, scalable network available to all parties in all languages. Google's main problems are (1) its lack of security, and (2) the imprecision of its search, which substitutes popularity for relevance. Both of these shortfalls are resolvable, the first by

integrating the CISCO Application Oriented Networking (AON) family of capabilities for secure content-based routing and global security access rules; the second by integrating IBM's Database 2 with OmniFind as an internal database standard for corporate and nongovernmental access.

The day of unilateral secret systems is over. DoD has begun to recognize that 90 percent of the content—and 90 percent of the capabilities—for achieving information superiority are in the private sector. The initiatives being taken by the Under Secretary of Defense for Intelligence are right on target, but need to be orchestrated to achieve information superiority in all languages.

CHAPTER 4

STATEMENT OF REQUIREMENTS

Global Access to Open Sources.

A major impediment to DoD and U.S. Government effectiveness in the Open Source Information (OSIF) and Open Source Intelligence (OSINT) arenas is the lack of a single system that can store all OSIF/OSINT funded by all elements of the government, while simultaneously offering a means of distributed search and retrieval from across all private and public databases that are not part of the U.S. intelligence community (and do not desire to be). OSIS-X will resolve this deficiency, and in adopting all relevant Intelink and OSIS meta-tagging standards, will allow for constant easy harvesting from OSIS-X all the way to the high side. The Under Secretary and the Defense Open Source Council (DOSC) have articulated a good first-ever definition of DoD mission-oriented needs for tailored OSIF/OSINT support to the COCOMs and the various defense elements.[87]

Among the desirable features that diverge from traditional U.S. intelligence community approaches to OSIF/OSINT are the following:

- Need near-real-time processing of all open sources in all languages;
- Translators need not be U.S. citizens if using cover support plans;
- Includes global access to subject matter experts who are not U.S. citizens;
- Includes commercial imagery and geospatial information;
- Includes offline gray literature as well as "street talk" and sermons; and,
- Must be shareable with NGOs and other foreign organizations.

Deep web content acquisition not available from commercial aggregators is a major aspect of the open source information

challenge. However, private databases, especially NGO databases, niche and mainstream publications, gray literature, sermons, and street talk, as well as new knowledge created by subject matter experts on demand, are part of the larger global pool. They can and must be addressed in at least 33 languages all the time, and in up to 185 languages some of the time.

Presently, there appear to be roughly $1.5B over 5 years in open source information contracts under disparate management across the COCOMs and the various elements of DoD. It is imperative that those contracts be brought under centralized oversight so that requirements can be deconflicted, standards established, best prices and practices understood, and—most important of all—deliverables brought together into OSIS-X and not buried within various "pits." Ideally, such contracts will inspire matching funding for DHS, and OMB eventually will prevail in its view that a national Open Source Agency, a sister agency to the Broadcasting Board of Governors and one independent of all Cabinet departments, is the best way to address national needs for both unclassified and sensitive information sharing.

Access to open sources is not achieved solely through physical contact or cash payment. Sharing begets sharing. The Silicon Valley Hackers Conference discussed this topic in the 1990s,[88] concluding that, for every piece of useful information that one posts on the Internet, 100 unsolicited pieces of related information come back, of which 10 are unique and useful. That is a 10:1 return on the sharing investment. OSIS-X will not only make sense of all that we can know and prevent dots from being dropped in the future, but it will create an information ecology, an environment in which information attracts more and more information, makes more and more sense, and ultimately changes the American way of war and the American way of commerce.

Geospatial Tagging and Visualization.

In 1988, at a meeting of the General Defense Intelligence Program (GDIP) taking place at USSOCOM, as the Marine Corps representative I stressed the need for geospatial tagging of all data collected by all disciplines, pointing out that automated all-source

fusion would not be possible until this became a pervasive practice. In 1992, at a meeting of the Council of Defense Intelligence Producers (CDIP) taking place at Offutt Air Force Base, Nebraska, the Marine Corps representative (Colonel Bruce Brunn, then Director of the Marine Corps Intelligence Center) said, "I don't care how much order of battle data you give me; if I cannot plot it on a map, it is useless to me."[89] We were both referring to 1:50,000 combat charts with elevation contour lines, the only acceptable resolution when you are an infantry commander trying to survive in defilade, or kill other people who are themselves using defilade to avoid artillery and direct fire.

Today, 17 years after Colonel Mike Pheneger, then J-2 of SOCOM,[90] and I made this an issue, we still do not have 1:50,000 combat charts for most of the Third World where S&R operations will take place and where UN forces are engaged in combat operations across 16 complex emergencies.[91]

There is good news, however. The National Geospatial Agency (NGA) has evolved toward a digital geospatial architecture, and Digital Terrain Elevation Data (DTED) are available at 10, 3, and 1 meter resolution, some Swiss cheese data gaps notwithstanding. It is now possible, if all data inherit geospatial tagging upon being entered into the system of systems, to move toward automated geospatial depictions of data from multiple sources in multiple languages. At the same time, the commercial geospatial industry has matured, and it is now possible to mirror NGA capabilities in the private sector.

We need two initiatives: First, we must demand geospatial tagging from all disciplines, including Human Intelligence (HUMINT). This will be aided by the emergence of locationally-aware devices, but needs flag-level attention now.[92] Second, we must fund commercial production of 1:50,000 combat charts for the UN combat missions that will eventually require the introduction of U.S. forces engaged in S&R activities. Figures 6 and 7 illustrate two alternative geospatially-based visualizations.[93]

There are numerous open source as well as proprietary visualization tools that can be applied. Figure 7 shows a depiction from one promising DARPA-funded source. There are others. We specifically avoid favoring any one visualization system—it is the

underlying data processing[94] which makes customized visualization possible for a wide variety of needs across the full spectrum of end-users.

Shareable situational awareness enables successful operations of distributed networked forces and their coalition partners. Experience from Operational Intelligence (OPINT) based experimentation during recent deployments to Afghanistan, Indonesia, and Iraq has highlighted the profound need for shareable situational awareness tools and visual representation methods to enable rapid sharing of complex critical data in a timely manner with multiple coalition partners. These capabilities are needed to support the difficult modern missions of distributed networked forces and their coalition partners in austere environments with challenging rules of engagement.

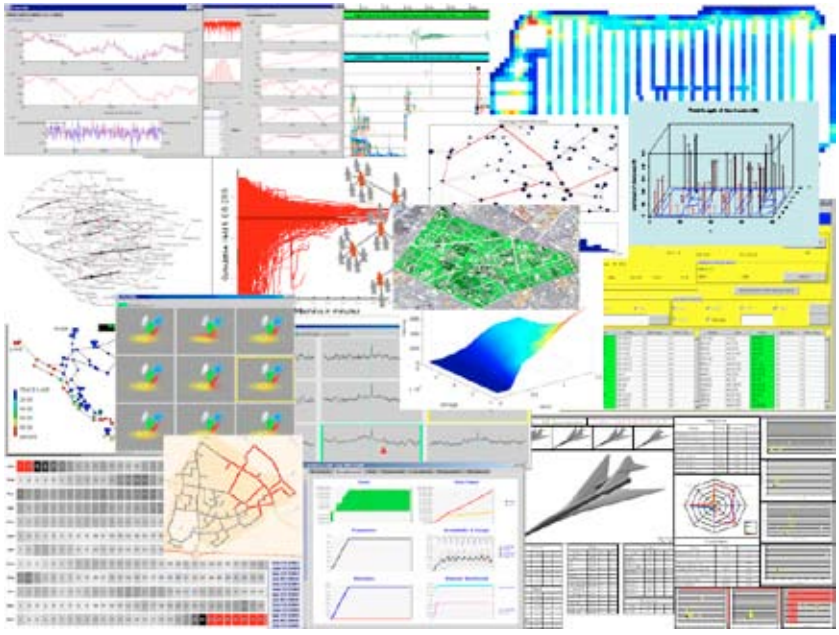


Figure 6. Alternative Visualization Options.

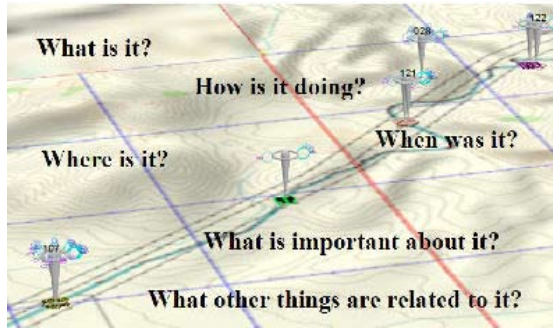
These kinds of depictions and the ability of varied parties to share near-real-time "looks" at trends, patterns, and emerging event sequences will be facilitated by embedding geospatial tagging attributes into all hand-held and other collection and reporting devices.

Same Data - Different Focus

General Concept Overview

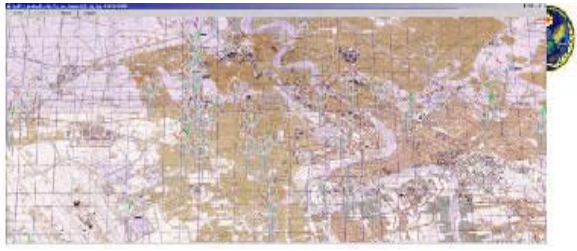
Events (incidents) and entities occur in space and over time.

There are multiple parameters of interest for each event/entity.



Shareable Situational Awareness

Figure 7. Other Visualization Options. (continued on next page).



Textual information can be turned on and off depending on use

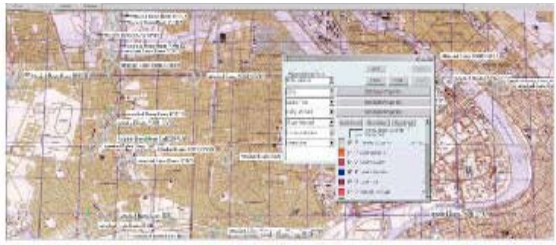


Figure 7. Other Visualization Options (continued from previous page)

Man-Machine Foreign Language Translation Network.

Machine translation, despite decades of effort, is in its infancy. While CYBERTRANS and SYSTRAN are useful in a limited sense, they are by no means adequate to the task of comprehensive near-real-time translation, nor even to the task of nuanced selection of materials for closer examination by humans. With Babylon Enterprise, they are helpful in providing "good enough" title and text translation for a human eye to evaluate possible utility, and they are also helpful in translating from English into foreign languages searchs for relevant documents across varied systems (e.g., SAP, Oracle, Siebel).

Online dictionaries, despite claims made by many promoters of these tools, are also in their infancy. Dramatic improvements are expected soon but not through the beltway bandits. We have found that personnel indigenous to the country where the target language is spoken can create really excellent online dictionaries at a fraction of the price demanded by beltway bandits, with the advantage of having nuanced terms and tailored specialty dictionaries included as a routine part of the development.

Where major gains can be made in the near term is in the exploitation of distributed human subject-matter experts with

native-level fluency. We must break out of the strait-jacket mind-set saying that only U.S. citizens with clearances can be used to do translations for national security or intelligence purposes. When it is the norm for most translations to be of unclassified and global piecemeal web-based material, for example, it makes sense to think in terms of translators in this specific order of utilization:

- Foreign indigenous personnel;
- U.S.-based native-fluency personnel;
- U.S. citizens with near-native fluency living overseas;
- U.S. citizens with clearances, including reservists working from home; and,
- U.S. citizens with clearances on site.

Open sources without near-real-time evaluation, gisting, extraction, or translations are of marginal value. There are four distinct time/cost paradigms in the foreign language arena, and our current practices do not manage the four adequately. We must avoid the temptation to demand the translation of everything. Translations are a complement to pattern and predictive analysis in the original language, and to gisting by experts with native-level fluency. We must focus on the wheat, not the chaff.

Analytic and Decision-Support Services.

In evaluating those who offer "analytic" services, they should always be asked to present their models for analysis. More often than not, they will not have any but will instead be relying on "bodies by the hour," doing cut-and-paste extraction and database stuffing. That is not analysis.

Key personnel being proposed as analysts must demonstrate, apart from the required educational and experience credentials, an ability to break down a problem, create and test hypotheses, construct a research argument or finding, and itemize essential elements of information that are missing and that could, if found, help resolve uncertainty.

There is no substitute for subject-matter experts (SME). However, the current practice is biased in favor of SMEs who are captive within vendor organizations, and consequently just one layer removed from the bureaucratic mind-sets they are supporting. There is also a bias toward SMEs that are U.S. citizens and have clearances. This is not the most effective means of understanding the real world. Instead, we must strike a balance in our outreach and integration by embracing:

- World-class experts regardless of nationality, hired one day at a time,
- World-class experts that are U.S. citizens without clearances,
- Retired government or private sector specialists, and
- Dedicated full-time analysts at the journeyman level.

If a vendor cannot readily identify the top 25 experts in the world on any topic, he or she is not ready to provide world-class support.

Statistical analysis and pattern or predictive analysis and trend detection are very important aspects of modern IO now that the center of gravity has shifted toward content analysis. The government should be very cautious in evaluating claimed capabilities where there is a heavy reliance on statistics packages or pre-packaged software. If the individuals contemplated for hire do not have a very advanced mathematical background (which includes multivariate analysis/ data mining), then they are just blind users of software they do not understand, the equivalent of a student using a crescent wrench without the slightest idea of the physics underlying mechanics.

One common mistake within IO is to substitute quantity for quality, and analyze chatter in relation to volume with no real opportunity for delving into the content. The best pattern and predictive analysis are done against unstructured multimedia data, in the original languages, with a global network of SMEs able to detect and highlight nuances in the context of the patterns found by automated analysis. Such capabilities are not linear in nature—they detect anomalous clusters, and they also flag vacuums, i.e., missing information that would normally be present.

Operational Open Source Software Collaborative Analytic Toolkits.

Many governments, including the United Kingdom, Norway, Israel, Germany, Brazil, and China are moving toward open source software instead of proprietary software as is offered by Microsoft, for three reasons: first, they feel they cannot impose on their citizens a requirement to buy proprietary software in order to read government documents; second, proprietary software is unaffordable at local levels trying to catch up to the national level's embrace of modern information technology; and third, proprietary software, Microsoft's in particular, is notoriously insecure.[95] Open source software, while its maintenance is not free, offers a lower total cost of ownership than proprietary software. DARPA STRONG ANGEL is on the right track. DHS, its state and local constituencies, and the NGOs merit DoD support in this area.

SILOBREAKER is used to obtain an unmatched combination of web-based access to tens of thousands of sources around the world, and the Elucidon suite of tools. The larger American and European information industry players—the ones created in the aftermath of World War II and in the heyday of mainframe computers that still dominate many of their operations, will be completely overshadowed—and many driven to bankruptcy—by the new secure Internet, OSIS-X, and SILOBREAKER-like capabilities that are now commoditized.[96]

Tactical Hand-Held Devices.

In the Third World, it will be the cell phone, not the personal computer, that drives micro-capitalism, informed democracy, and localized access to the global grid. The World Bank is usefully funding millions of Motorola cell phones adapted to World Bank specifications to be distributed in the Third World at a cost of under $30 each. It is important to note that in areas where individuals are living on $2 a day, this cost, while trivial to us, is to them as relatively large an investment as the average American might make in his or her personal automobile.

The tactical computers commissioned by USSOCOM, which are hand-held computing devices, are at the other end of the spectrum of technical sophistication. Between them are commercial specialized hand-helds that include locational awareness, cameras, and the capability to report ground truth information upwards by use of a simple template and to pull down tailored information whose relevance is enhanced by the locational awareness of the device ("show me car rental agencies within a mile of my location" or "show me a 1:50,000 depiction of the other side of that hill, 500 meters away").

Within complex emergencies in particular, where U.S. forces will be heavily interactive with NGOs as well as coalition law enforcement personnel and others, it is the tactical hand-held device that will bear the greatest burden in IO. Such devices, in addition to being locationally aware, must also be aware of who else is in their area by classification (NGO, U.S. Government, etc.), and will, by virtue of this knowledge when combined with localized content-based routing, be able to exchange "dots" locally without having to suffer the long reach-back and delayed processing characteristic of today's stovepipes.

Precision Strategic Communication.

Novices do broadcast press releases. Journeymen do specialized lists. The real masters, however, know how to reach key communicators in any domain, any country, "by name." Moreover, they employ *individualized messages*, informed by values-based biographies and sophisticated social network analysis.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

IO and the Fate of the Nation.

The fate of the nation rests on IO and how we execute the IO mission in the next several years. There are three parts to that mission: Strategic Communication (the message), OSINT (the reality), and JIOCs (the technology). Figure 8, duplicating Figure 1 shown in Chapter 1, illustrates our vision of how commercial implementation, funded and overseen by DoD, could benefit the information health of our nation.

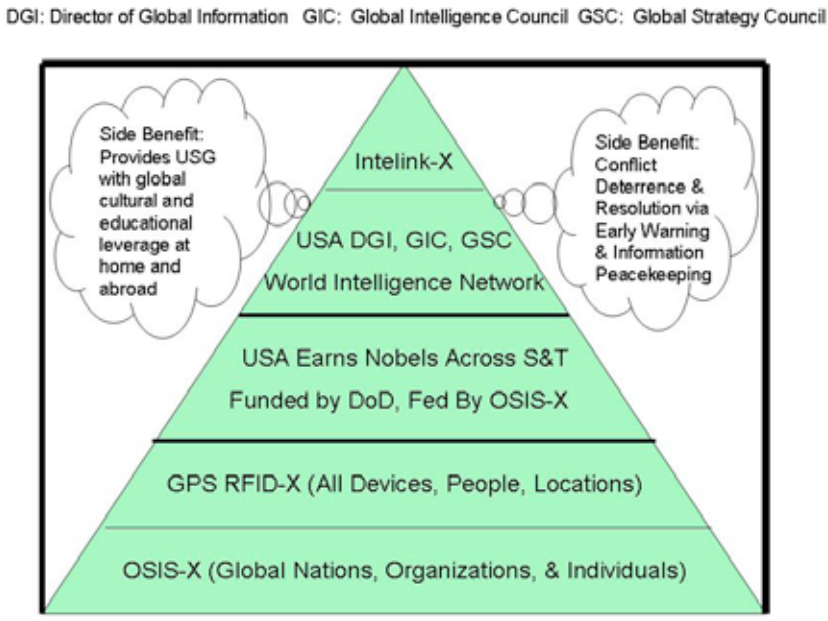


Figure 8. Creating the World Brain for U.S. Benefit.

Each of the layers shown in Figure 8 is both achievable in the near-term, and of inestimable value in revitalizing national education, R&D, and intelligence. We describe each very briefly below. If Google can be co-opted, such improvement will happen fast.

OSIS-X. The commercial implementation of OSIS discards the old legal and security mind-sets and moves directly to commercial-level

openness combined with commercial-level security. By migrating the "look and feel" of OSIS and Intelink to the commercial sector and by adopting the excellent meta-tagging philosophy of both Intelink and the federal data management and national information exchange models, OSIS-X provides all federal agencies and all state and local authorities with an open but secure "leap ahead" approach to information-sharing.

GPS RFID-X. The government has been slow to adopt both Radio Frequency Identification (RFID) and mandatory geospatial tagging such as XML-Geo. This next level up will provide incentives for data that is properly tagged with geospatial as well as time and date information, and will enable "Green Lane" speed of processing for compliant sectors (e.g., cargo ships with containers so equipped).

Scientific and Technical (S&T) Revitalization. The Defense Technical Information Service (DTIC) does information monitoring in support of defense S&T, but its access to foreign language information, where most of the real innovation is occurring, is virtually nonexistent. USDI's initiative, when implemented commercially, will open the floodgates of access to foreign S&T, and will lead to a resurgence of Nobel Prizes across the U.S. S&T community.

Global Scope. A Director of Global Information (DGI), perhaps sitting on top of a government-sanctioned skunk works,[97] and orchestrating a multinational Global Intelligence Council (GIC) and a multinational Global Strategy Council (GSC), will take American understanding and influence to a new level of play.

Intelink-X. Multilateral classified information-sharing will occur soon. In an era when information converted into intelligence and knowledge is a substitute for wealth, violence, energy, water, and everything else, only the the United States has the power to execute the practical vision represented by Intelink-X. DoD is the catalyst for its achievement.

The 21st century, unlike the 20th, demands a sophisticated and constant application of all the sources of national power. It is no longer sufficient to have the strongest largest military or the strongest largest economy. Indeed, under the pressures of the trade and budgetary deficits and GWOT, there are those who say that America is "running on empty"[98] and at risk of a strategic collapse.

Modern IO is the seed for a total transformation of the American way of war, a new American way that practices information peace-keeping and reflects a new commitment by America to stabilize the world intelligently rather than violently. It is a holistic mission that must be accomplished by the J-3 using a civil affairs mind-set, with the J-2 limited to internal validation and support. There are not enough guns on the planet to force our will upon another or to protect our quality of life for future generations.[99] IO is the new way of war and of peace.

The USDI strategy of integrating Strategic Communication (the message), OSINT (the reality) and JIOCs (the technology) is constructively transformative. This strategy must be understood by all concerned, and it must be managed as a whole, not as discrete financial hand-outs in exchange for limited localized mission support. While Strategic Communication is the mission to be supported, OSINT must come first. Without global OSINT, 24/7, down to the neighborhood, village, tribal, and provincial levels, we will not be able to do the Intelligence Preparation of the Battlefield (IPB) necessary to deliver effective messages "by name," nor to act intelligently, using all the instruments of national power in every clime and place.

Nor can we do this alone. We can fund the architecture and we can offer other legitimate governments and organizations an opportunity to participate, but we must do so with a willingness to listen to what we hear, and a willingness to change our behavior where it makes sense to do so in keeping with our objective of stabilizing and reconstructing the world. Seven generations from today, what will we have wrought?

Recommendations.

Creation of a National Information Council (NIC), coequal to the National Security Council (NSC) and the National Economic Council (NEC), is necessary if the White House is both to harness the distributed intelligence of the nation and the world, and to achieve its objectives in public diplomacy, strategic communication, interagency information-sharing and collaboration, a renaissance in public education, and the resurrection of national research. One

priority should be the orchestration of information technology and informatics initiatives from the various elements of the government (e.g., the National Science and Space Administration [NASA] and the Defense Advanced Research Projects Agency [DARPA]) so as to accelerate the application of information advances to conflict prevention and resolution, and to the creation of wealth.

*Congress***.** Intelligence and information-sharing are inherently critical aspects of all government operations. Each congressional committee should create a Subcommittee on Intelligence and Information Operations (I2O). The chair and ranking minority member of each of these subcommittees, or their designated representatives, should in turn comprise a new Special Committee on I2O that has oversight over the national Open Source Agency and information operations across all federal agencies, and a special relationship with the respective Intelligence Committee, which shall continue to focus on classified sources and methods.

*White House***.** Expand the extraordinary earth science information-sharing initiative to include the sharing of information about disease, crime, poverty, and other nontraditional threats to our national security and prosperity.

*Director of National Intelligence***.** Free the Open Source Agency from U.S. intelligence community affiliation or direct oversight. Instead, follow the expert recommendation that it be a sister agency to the Broadcasting Board of Governors under Department of State auspices. Fully fund the Open Source Information System–External (OSIS-X) as a commercial venture open to all legitimate governments, nongovernmental organizations, and private sector corporations, universities, and groups.

*Department of State***.** Establish an Office for Information-Sharing Treaties and Agreements. This small office of perhaps 10 individuals, led by accredited diplomats, would negotiate information-sharing treaties with nations, and information-sharing agreements with organizations, with the immediate objective of extending data and information standards to all participants. All embassies should be integrated into it.

*Department of Defense***.** Rapidly establish JIOCs within each Combatant Command (COCOM) as well as a DoD JIOC, while establishing two new Combatant Commands: one for I2O, and one

for S&R. Integrate the Strategic Decision Support Center envisioned by Captain Scott Philpott, USN, into COCOM I2O. Redirect the USSTRATCOM toward the oversight and orchestration of Big War. COCOM I2O should have oversight of the Defense Information Systems Agency (DISA), DTIC, and the various departmental-level intelligence organizations. It should also have authority over the JIOCs at each COCOM analogous to that retained by the services over ground, sea, and air components. The I2O needs of policy, acquisitions, logistics, and operations should be deliberately attended to, with OSINT as the source of first resort (always copied simultaneously to the relevant all-source intelligence provider). Place the National Guard under the operational oversight of the U.S. Northern Command (USNORTHCOM), and begin the process of redirecting the Guard toward a true Home Guard role in which it has specialized units for medical, fire, police, and disaster-relief engineering that are suitable equally for homeland security duties as well as support for global S&R operations. Direct DARPA to establish an S&R Directorate charged with developing information solutions for conflict prevention and resolution, and the creation of indigenous stabilizing wealth.

*General Services Administration (Office of Intergovernmental Solutions)***.** Sponsor a summit and an ongoing Wiki web site on the four "opens" that will energize information-sharing in the future: 1. Open Source Software; 2. Open Source Information; 3. Open (Electromagnetic) Spectrum; and 4. Open Hyperdocument System (OHS).

*Department of Commerce***.** Issue an antitrust waiver for a private sector OSINT skunkworks that will fully integrate and test all available open sources, softwares, and services. This skunkworks will accelerate the development of open common standards for information-sharing that will be truly worldwide, with the added advantage of developing commercial alternatives for the sharing of secret information across national, cultural, and government-to-nongovernment boundaries on a by-name, by-paragraph basis.

*Department of Justice***.** Submit proposed legislation to Congress mandating the open disclosure and stability of Application Program Interfaces (API) within all software purchased by the government and offered for sale within the United States. Demand that all

software have transparent and stable API by 2008, or be banned from the Federal marketplace. This is the only way to achieve our full IO potential.

*Open Source Agency***.** Execute the 100-day start-up plan that already has been drafted and is easily achievable by drawing on the OSINT pioneers across the U.S. Army and in other services to include:

1. IO/OSINT training program, resident, mobile, and remote learning;
2. IO/OSINT help desk, 24/7, multilingual;
3. IO/OSINT global translation web in all languages, including support of 911 calls;
4. IO/OSINT historical and cultural "Manhattan Project," starting with Iran;
5. OSIS-X with DoD first, then NATO, then each COCOM's coalition partners;
6. Grant free OSIS-X access to all NGOs and academic institutions;
7. Create a living directory of top 100 experts on each country and topic;
8. Create Texas Early Warning Center;
9. Create New York Corporate Warning Network;
10. Implement Digital Marshall Plan, using residual capability in abandoned satellites; and
11. Sponsor a University of the Republic to foster information-sharing.

APPENDIX

ANALYTIC MODELS FOR MODERN IO

There are numerous analytic frames of reference and methodologies, and we strive to recognize and exploit them all, as appropriate. Here we wish to put forward just two (Figures 10 and 11) that we have found useful and relevant to the challenges facing STRATCOM and SOCOM, among others.

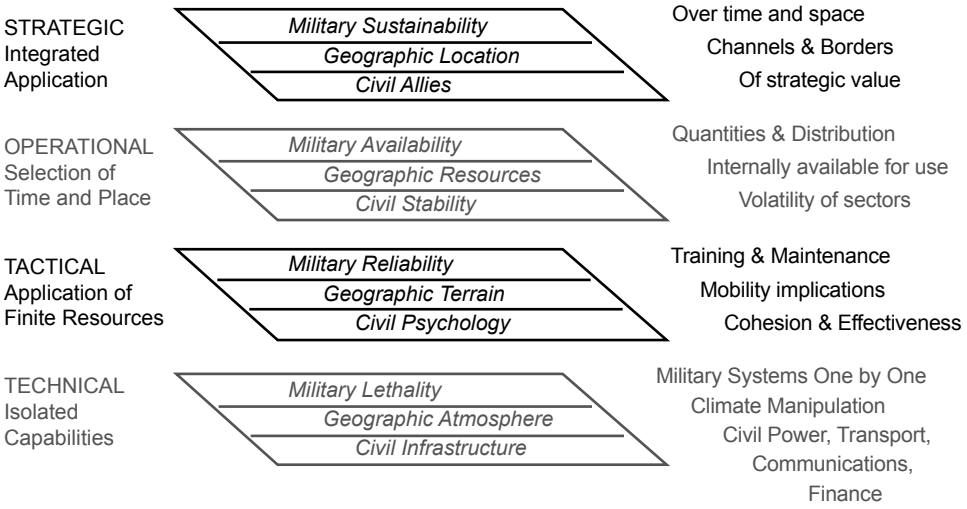


Figure 10. Analytic Domains and Levels of Analysis.

It has been our experience that too many so-called analytic services limit their efforts to database stuffing and summarization. As shown in Figure 10, there are four levels of analysis—strategic, operational, tactical, and technical; the threat, and consequently the needed message, changes at each of these four levels. By distinguishing between military, geographic, and civil domains, by understanding the uniqueness of each of the four levels of analysis, and by placing particular emphasis on the civil domain, we can enhance our analytic statecraft. The latter would entail a strong focus on civil psychology, on indicators of civil stability, and on influences relevant to civil allies (and competitors), in combination with an understanding of the civil infrastructure, and all forms of communication in the target societies.

	Political-Legal	Socio-Economic	Ideo-Cultural	Techno-Demographic	Natural-Geographic
Perception	Isolation of elites; inadequate intelligence	Concentration of wealth; lack of public disclosure	Conflicting myths; inadequate socialization	Acceptance of media distortions; inadequate education	Reliance on single sector or product; concentrated land holdings
Identity	Lack of elite consensus; failure to define priorities	Loss of economic initiative; failure to do balanced growth	Loss of authority; failure to provide and honor national myth system	Failure to accept and exploit new technologies and new groups	Failure to integrate outlying territories into national system
Competence	Weak or inefficient government; too much or too little bureaucracy	Break-down of fiscal, monetary, development, or welfare policies	Humiliation of leaders; loss of confidence by population	Failure to enforce priorities, with resulting loss of momentum	Failure to prepare for or cope with major national disasters
Investment	Ego-centric or parochial government	Excessive or insufficient mobility; lack of public sector	Cynicism; opportunism; corruption	Failure to nurture entrepreneurship or franchise all groups	Failure to preserve or properly exploit natural resources
Risk	Elite intransigence; repression; failure to adapt	Failure to deal with crime, especially white collar crime	Failure to deal with prejudice; desertion of intellectuals	Failure to develop national research & development program	Failure to honor human rights; failure to protect animal species
Extroversion	Ineffective tension management; failure to examine false premises	Structural differentiation; lack of national transportation network	Elite absorption of foreign mores; failure to deal with alienation	Failure to develop communications infrastructure, shared images	Failure to explore advantages of regional integration
Transcendence	Foreign control of government; arbitrary or excessive government	Loss of key sectors to foreign providers; loss of quality control	Media censorship; suppression of intellectual discourse	Failure to control police, army, or terrorists; failure to employ *alphas*	Failure to respect natural constraints or support organic growth
Synergy	Failure to assimilate all individual or respond to all groups	Status discrepancies; lack of economic motivators	Absence of sublimating myths; failure of religion	Failure to provide program and technology assessment	Failure to distribute benefits between urban and rural
Complexity	Garrison, industrial, or welfare states	Unstable growth; excessive defense spending	Cultural pre-disposition toward violence	Excessive urbanization, pollution, or development	Lack of land for expansion; inefficient use of land

Figure 11. Framework for Predicting and Understanding Revolution.

Our second analytic frame of reference (Figure 11) combines a deep understanding of human psychology and sociology with a suitably complex yet refined understanding of the dimensions of revolutionary change in any nation-state, tribe, or neighborhood. Analysis of emerging and unconventional threats is not about traditional orders of battle, but rather about the psychology of the individual and the sociology of the substate group. It is about connecting ideas and people.

ENDNOTES

1. DIME: Diplomatic, Information, Military, Economic.

2. Although reformists have called for a unified national security budget process, this is still not practiced. The diplomatic budget (Program 150) and the military budget (Program 50) are devised in isolation from one another, while the information and economic budgets are scattered across multiple jurisdictions. Considerable savings, and a considerable enhancement of U.S. national security as well as national competitiveness, could be achieved if there were a unified national security planning, programming, and budgeting system (PPBS) that integrated both acquisition and operational campaign planning across diplomatic, information, military, and economic jurisdictions; and if "total information awareness" were centered on public information using Google and other available open systems, rather than being centered on secret information and closed intelligence systems that lack access to 90 percent of the relevant information.

3. Dr. Stephen Cambone articulated this requirement in a speech to the Security Affairs Support Association (SASA), the premier forum for senior executives in both government and industry who are engaged in intelligence support operations. See full text at *www.oss.net/extra/news/?id=2354*, where additional commentary is provided, and also at *www.oss.net/extra/news/?module_instance=1&id=2369*.

4. Alvin and Heidi Toffler, *PowerShift: Knowledge, Wealth, and Violence at the Edge of the 21st Century*, Bantam Books, 1990, p. 86. The Tofflers are investigative journalists and researchers at heart, and tend to do direct interviews and exploit raw information sources rather than secondary sources. They complement and are in total harmony with such other extraordinary current works as Thomas Stewart, *The Wealth of Knowledge: Intellectual Capital and the Twenty-First Century Organization*, Currency, 2001; and Barry Carter, *Infinite Wealth: A New World of Collaboration and Abundance in the Knowledge Era*, Butterworth Heinemann, 1999.

5. Their discussion of knowledge in relation to violence is contained in *War and Anti-War: Survival at the Dawn of the 21st Century,* Little Brown & Company, 1993, where the chapter on "The Future of the Spy" provides the first major public discussion of "the rival store" that focuses on open sources of information in all languages. They also addressed this theme when speaking in 1993 to the second annual international conference on "National Security & National Competitiveness: Open Source Solutions," in Washington, DC, November 2, 1993. The complete text of their remarks to this audience of over 800 predominantly U.S. military officers is available online at *tinyurl.com/dzwbz*.

6. *Supra* note 2.

7. Both reports are downloadable at the Defense Science Board web site, under Reports, at *www.acq.osd.mil/dsb/reports.htm*. The third DoD publication that underpins this monograph is Deputy Undersecretary of Defense for Homeland Security Gordon England's *Strategy for Homeland Defense and Civil Support*, June 2005, available online at *www.defenselink.mil/news/Jun2005/d20050630homeland.*

pdf. Careful reading of these reports will document two critical strategic and transformative themes common to all three: (1) information-sharing, exploiting all sources in all languages all the time, is the central tenet of defense in the age of information; and (2) nongovernmental organizations external to the U.S., and county-level law enforcement and civil organizations at the lowest level of the U.S. domestic governance hierarchy, must be included in defense information-sharing, at a cost they can afford (which is to say, at almost no cost to them) for access to "the network." This makes it clear that classified networks are not, repeat, not the answer to the larger challenge of global information monitoring and sharing.

8. The ideal approach to global information capture and exploitation is one in which diplomatic arrangements (the negotiation of information-sharing treaties with nations and information-sharing agreements with organizations) are implemented by the military using the civil affairs model, under J-3 operational control. Only when the information is "inside the wire," should it be subject to J-2 quality control and oversight.

9. One of the most important lessons learned from the GWOT is that intelligence is the smallest part of the information-sharing challenge, although also the most difficult to break out of the stovepipes. External open sources of information, operational traffic, logistics information, and acquisition capabilities and countermeasures information are all vital parts of the IO mosaic. Novices argue about sharing classified information; mid-level experts argue about U.S. Government interagency information-sharing; the real masters understand, as the Swedes have taught us, that the "endgame" in IO is about multinational, multiagency, multidisciplinary, multidomain information-sharing, M4 IS. As the Jolt cola commercial says, "Dare to want it all." For a report on the 3rd Annual Peacekeeping Intelligence Conference in Stockholm, Sweden, December 4-5, 2004, site of the first recorded mention of M4 IS, see the trip report at *tinyurl.com/a4f4r*.

10. There are 33 core languages (Arabic, Aramaic, Berber, Catalan, Chinese, Danish, Dari, Dutch, English, Farsi, Finnish, French, German, Indonesian, Irish, Italian, Japanese, Korean, Kurdish, Kurmanji, Norwegian, Pashto, Polish, Portuguese, Russian, Serbian, Spanish, Swedish, Tamil, Turkish, and Urdu) within which Arabic has at least 12 nuanced variants: *Andalusi Arabic* (extinct, but having an important role in literary history); Egyptian Arabic (Egypt), considered the most widely understood and used "second dialect"; Gulf Arabic (Gulf coast from Kuwait to Oman, and minorities on the other side); Hassaniiya (in Mauritania); Hijazi Arabic; Iraqi Arabic; Levantine Arabic (Syrian, Lebanese, Palestinian, and western Jordanian); Maghreb Arabic (Tunisian, Algerian, Moroccan, and western Libyan); Maltese; Najdi Arabic; Sudanese Arabic (with a dialect continuum into Chad); and Yemeni Arabic.

11. Machine translation and online dictionaries are completely inadequate to this challenge at this time, as are the limited number of U.S. citizens eligible for clearances. However, it is possible, if we break away from the rigid obsession with using only U.S. citizens with clearances, to create a global network of machine translation, innovative tailored online dictionaries; and a very broad network of

near-real-time human monitors, reporters, and translators who post material to the web as it becomes available, with translations and subject-matter annotations. The key here is to make the network multinational rather than unilateral.

12. The I in JIOC is for Intelligence, the C can stand for Center or Command, depending on how the COCOM wants to adapt the concept. Some, like EUCOM, appear to desire a command with all the authorities inherent in command, while other COCOMs are more comfortable with it being a center, so they do not have to tackle the challenges associated with breaking down the stovepipe authorities that plague the COCOMs. USDI's intent appears to be the establishment of a functional intelligence construct similar to the Joint Force Air Component Commander, JFACC, or Ground Component Commander, GCC, who would have all the authority to conduct the fight for knowledge, to include the protection component of the fight for information. While some interpret the I as standing for Information, or Interagency, USDI's intent appears to be for it to represent Intelligence, but in the broadest interpretation of the word, embracing all available information in all languages and at all levels of classification across all mission areas.

13. Peter Drucker, writing in *Forbes ASAP* on August 24, 1998, at p. 46:

> The next information revolution is well under way. But it is not happening where information scientists, information executives, and the information industry in general are looking for it. It is not a revolution in technology, machinery, techniques, software, or speed. It is a revolution in CONCEPTS. So far, for 50 years, the information revolution has centered on . . . the "T" in IT. The next information revolution asks, What is the MEANING of information, and what is its PURPOSE? And this is leading rapidly to redefining the tasks to be done with the help of information, and with it, to redefining the institutions that do these tasks. . . . We can already discern and define the next . . . task in developing an effective information systems for top management: the collection and organization of OUTSIDE-focused information.

14. The Report of the Independent Commission on the National Imagery and Mapping Agency, 2000, includes the following statement in the Foreword: "The Commission validates the charge that the Intelligence Community is "collection centric," thinking first of developing and operating sophisticated technical collection systems such as reconnaissance satellites, and only as an afterthought preparing to properly task the systems and to process, exploit, and disseminate the collected products." The report goes on to provide a brutally detailed indictment of decades of neglect for "sense-making" tools. View at *www.fas.org/irp/agency/nima/commission/toc.htm*.

15. Steve Emerson, *American Jihad: The Terrorists Living Among Us*, Free Press, 2002; and Yossef Bodansky, *Bin Laden: The Man Who Declared War on America*, Forum, 1999. Although *American Jihad* was published in the immediate aftermath of September 11, 2001, Steve Emerson had been briefing this message since 1994, when he produced a 1-hour special documentary for Public Broadcasting

Corporation (PBS) that displayed covert videos of imams on U.S. soil calling for the murder of Americans. Bodansky, then a senior staff director on the Republican Task Force on Terrorism on Capitol Hill, was ignored on the Hill, and despite his book being a *New York Times* #1 Bestseller, was ignored across the bureaucracy as well. "Mind-set," as so many have documented, is a very powerful filter, able to block very strong signals if they are inconsistent with the receiving person's preconceived notions.

16. Michael A. Turner, "Intelligence Reform and the Politics of Entrenchment," *International Journal of Intelligence and Counterintelligence*, Vol. 18, No. 3, Fall 2005, pp. 383-397, provides an objective and well-documented analysis of how vested interests prevailed, and true intelligence reform, including the all-important changes in mind-set and culture, was blocked. This reference is not online. For a shorter commentary that distinguishes between reactionary, evolutionary, and revolutionary intelligence reform, see Robert David Steele, "Intelligence Affairs: Evolution, Revolution, or Reactionary Collapse?" *International Journal of Intelligence and Counterintelligence*, forthcoming, at *tinyurl.com/8e6wx*. Additional references are at *www.oss.net/extra/news/?module_instance=1&id=1334*.

17. As of July 2005, the Director of National Intelligence (DNI) was said to be considering a Federally-Funded Research and Development Center (FFRDC) for OSINT. This may help CIA address its own internal needs, but it will not address the broader needs of DoD, or any other U.S. Government agency including Commerce, Education, Environmental Protection Agency, Interior, and Justice, among others, nor will it be responsive to operational or tactical levels of command and staff operations. As of September 14, 2005, there were unconfirmed reports that the DNI has realized that an independent national Open Source Agency, as we have long recommended, is actually essential to his success, and that he has asked Dr. James Billington, Librarian of Congress and veteran of the original Office of Strategic Services, to serve as the founding director of the OSA. If true, this is an inspired decision and choice.

18. As this monograph goes to press, the news media are delving into reports that "Able Danger," a data-mining and sense-making endeavor alleged to have been managed in the Tampa area, identified three of the 9/11 hijackers a year prior to 9/11, but that this information was not shared with the FBI because military lawyers and managers believed that they were not allowed to collect information on U.S. citizens or green-card holders. There were two important areas of ignorance among those making that decision, ignorance that persists today at USNORTHCOM and elsewhere: (1) visa holders are not U.S. citizens or green-card holders and are fair game; and (2) overt information is not proscribed by EO 12333. Commands are free to collect overt legally available public information on anyone, including U.S. citizens. Open source information can be converted into open source intelligence without violating any privacy or regulatory constraints, and it is therefore an essential foundation for domestic security operations. It can provide a basis for alerting appropriate authorities who can then exercise their legal powers to obtain subpoenas or begin surveillance under established

legal mandates and protocols. DoD can and should be the lead on global overt information monitoring, including within the homeland. Where DoD needs to improve is in its mind-set and knowledge of the law. DoD must err on the side of excessive sharing, not on the side of inappropriate concealment of overt knowledge.

19. USSOCOM is the only element of the U.S. Government that has been consistently innovative and transformative in OSINT support to both all-source intelligence and to operations and logistics.

20. Under USDI leadership, the Defense Open Source Council (DOSC) has completed its investigation and made recommendations that have been coordinated at the flag level across all services and agencies of DoD. A fine start, DoD nevertheless continues to lack a Combatant Commander for Intelligence. It could also benefit from redefining USDI to make it clear that USDI is responsible for all information as well as intelligence. It is essential that operational, logistics, acquisition, and other information be managed as a coherent whole, not in isolation from classified intelligence. Sharing and sense-making, not hoarding and secrecy, are the watchwords today.

21. USSTRATCOM has a Joint Information Operations Center (JIOC) with a responsibility for integrating IO across all military and operational areas. See note at *www.stratcom.mil/FactSheetshtml/Jointpercent20Infopercent20Operations percent20Center.htm*. USSOCOM is taking the lead for USDI in building a Joint Interagency Collaboration Center (JICC) that is intended to create a rapidly replicable set of technologies that can be migrated to the other COCOMs and—ideally—to DHS constituents and to the NGOs. The National Guard activities in various states do not appear to have a coherent concept of operations, nor do they appear to have any larger concept for being connected to a DoD-DHS continuum of IO sources and services. The Guard is well-qualified to man information-sharing facilities, but it is not qualified to design or build them on behalf of the states.

22. The seminal work in the field, the classic report on UN success "against all biases," is told by A. Walter Dorn and David J. H. Bell in "Intelligence and Peacekeeping: The UN Operations in the Congo, 1960-1964," *International Peacekeeping*, Vol. 2, No. 1, 1995, reprinted as Chapter 15 in *Peacekeeping Intelligence: Emerging Concepts for the Future*, OSS, 2003.

23. Deputy Secretary General Louise Frechette, former Deputy Minister of Defence in Canada, assuming her new role in March 1998, was appalled at the lack of decision-support—another term for the intelligence cycle—within the Secretariat and Offices reporting directly to the Secretary General. She appears to be a compellingly effective but largely anonymous force in support of UN PKI. Completing the circle of sensible military professionals advising the Secretary General were Major General Frank van Kappen, Marine Corps of the Royal Netherlands Navy, who, in his own words, "failed" as Military Advisor to the Secretary General from 1995 to 1998 but, in fact, succeeded in setting the stage for his successor, Major General Patrick Cammaert. Secretary General Kofi Annan

commissioned a Panel on U.N. Peace Operations, led by Mr. Lakidar Brahimi of Algeria. The Brahimi Report is a revolutionary document, which recognizes that the ultimate tool necessary to help the United Nations succeed in saving succeeding generations from the scourge of war is intelligence—actionable information. While the Brahimi Report recommendations were resisted and not fully implemented, they paved the way for the findings of other reports, notably the Millennium Report and the report of the High-Level Panel on Threat, Change, and Challenge, *Creating a More Secure World, Our Shared Responsibility*. Lieutenant General (Ret.) Brent Scowcroft was the U.S. representative to the latter panel. During this period, an edited work, *Peacekeeping Intelligence: Emerging Concepts for the Future*, OSS, 2003, was published, and was soon on display in the lobby of 1 UN Plaza. Copies were widely distributed by General Cammaert to Force Commanders and UN agency heads. Reporting to the 3rd annual PKI conference in Stockholm in December 2004, General Cammaert said, "Intelligence is no longer a dirty word within the UN bureaucracy."

24. "Peacekeeping Intelligence: Leadership Digest 1.0," a distillation of the book, *Peacekeeping Intelligence: Emerging Concepts for the Future* (OSS, 2003), contains a complete discussion of PKI at the various levels and across collection, processing, analysis, and security. It can be found online at *tinyurl.com/cdd5h*. The book is available to individuals at Amazon.com. War colleges may buy the book at half-price from the publisher when ordering a minimum of 96 books, or 6 boxes.

25. Rwanda and now Sudan remain examples of UN and Western failures to intervene, in part because available public intelligence has not been sufficient to compel public policy. For a heart-rending account of the failure of the UN mandate and the UN bureaucracy in Rwanda, see Lieutenant General Romeo Dallaire, Canada, *Shake Hands With The Devil: The Failure of Humanity in Rwanda*, Random House, 2003. For a learned discussion of both how easy it is to acquire early warning of genocide, and how to take practical action to prevent it, see John G. Heidenrich, *How to Prevent Genocide*, Praeger, 2001; and also the web site, *www.genocidewatch.org*, where Dr. Gregory Stanton, a foremost authority, discusses the eight stages of genocide, including the stages preceding genocide where early warning is achievable.

26. Robert B. Oakley, Michael J. Dziedzic, and Eliot M. Goldberg, contributing editors, *Policing the New World Disorder: Peace Operations and Public Security*, NDU, 1988, is the source of the criticism of UN law enforcement cadres, and the definitive report on the "cop gap" in peacekeeping operations. The best available book on the recurring failures of both UN and Western interventions in failed states is William Shawcross, *Deliver Us From Evil: Peacekeepers, Warlords, and a World of Endless Conflict*, Simon & Schuster, 2000. The best documented inventory of "gap" nations is Robert Young Pelton, *The World's Most Dangerous Places*, Harper, 2003. Although no longer in print and now a collector's item, but visible in Pelton's lectures on the real world, *Map of World Conflict and Human Rights*, from Leiden University and the Goals for Americas Foundation, remains an exemplary depiction of all that ails the world, where most conflict is substate conflict, not interstate.

27. Colonel Mike Pheneger, USA, then J-2 for the U.S. Special Forces Command, and the author, then Special Assistant and also Deputy Director of the U.S. Marine Corps Intelligence Center (today a Command) catalogued the 1:50,000 combat chart deficiencies in 1988. The author got maps added to the Foreign Intelligence Requirements and Capabilities Plan (FIRCAP) in 1992, but today, 13 years later, we still do not have 1:50,000 combat charts "on the shelf" because of a continued emphasis on digital products that will not operate with a bullet hole through their display screens. There are two bright spots: (1) we have Digital Terrain Elevation Data (DTED) for most of the world via the shuttle mission, although it tends to look like Swiss cheese due to multiple failures; and (2) at least one commercial vendor has NGA-level equipment and the ability to produce maps on a 24/7 basis, with a single 1:50,000 combat chart costing $17,500. This is one problem that money *can* solve, beginning with each of the 16 most critical complex emergencies where multinational forces are in harm's way.

28. We began calling for substate and nonstate Orders of Battle (OOB) in 1994. Both governments and vendors have failed to rise to the challenge. PMCs now join terrorists, criminals, "random actors," and radicalized religious groups as belligerents whose key personnel and capabilities must be tracked. Fortunately, it is now possible to create such OOB on the fly, and without recourse to the commercial databases that have minimal foreign content and focus primarily on business needs. A global network of "virtual" defense and law enforcement attaches is in place and highly responsive, and can produce tailored "on demand" OOB for a fraction of the cost of the "gold license" fees that the commercial aggregators demand. Put bluntly: for $1M a year, DoD can get a gold license for content that will be useful 10 percent of the time, or it can obtain between 40 and 100 unique tailored products that do not exist in the commercial databases. DoD should buy information "by the drink," not on a gold license basis. Commercial and academic aggregators mislead their clients when selling their access. They are largely focused on English-language information that is of business value. They have not invested in historical, cultural, social, ideological, criminal, and environmental data, and are not competitive with true multilingual tailored sources that can meet our demands "by the drink."

29. Huge Smith, "Intelligence and UN Peacekeeping," *Survival*, Vol. 26, No. 3, Autumn 1994, reprinted as Chapter 14 in *Peacekeeping Intelligence: Emerging Concepts for the Future*, OSS, 2003.

30. The traditional relationship between NGOs and the U.S. intelligence community, including the DIA, is completely unacceptable. The U.S. focus is on sanitizing classified information of marginal value, or stone-walling the NGOs completely after first getting everything the NGOs have to offer. A much more productive approach is to establish jointly shared requirements, to share what each knows via overt means, and to gradually expand the circle of participants in an overt network so that more and more distinct entities are both contributing original information, and drawing upon the aggregate information, to which DoD can add considerable value by applying generic sense-making tools.

31. Alvin and Heidi Toffler understood the importance of this concept when it was presented to them in 1992, and spent five of 12 pages of their chapter on "The Future of the Spy" covering "The Rival Store" as created by OSINT. These ideas evolved further toward 1994, and were addressed in "Talking Points for the Director of Central Intelligence" dated July 20, 1993, subsequently published in *Proceedings of the Second International Symposium* on "National Security & National Competitiveness: Open Source Solutions," Washington, DC, November 2-4, 1993; "ACCESS: Theory and Practice of Intelligence in the Age of Information," October 26, 1993; "Reinventing Intelligence: Holy Grail or Mission Impossible," *Periscope*, *Journal of the Association of Former Intelligence Officers*, June 1994; and a keynote speech to the Association for Global Strategic Information (AGSI) in Germany titled "ACCESS: Theory and Practice of Competitor Intelligence," printed in the *Journal of AGSI* in July 1994. All are at *www.oss.net* and easily found using the Google Super Search feature.

32. At *www.usip.org/virtualdiplomacy/publications/papers/virintell.html*, and published with the same title 2 years later in the *Journal of Conflict Resolution* at *tinyurl.com/8teqf*. Other later chapters and articles addressing the common theme of information strategy in relation to national security included "Information Peacekeeping: The Purest Form of War," Chapter 7 in Lloyd J. Matthews, ed., *Challenging the United States Symmetrically and Asymmetrically: Can America Be Defeated?* Carlisle, PA: Strategic Studies Institute, U.S. Army War College, July 1998, pp. 143-171; "Information Peacekeeping: The Purest Form of War," in Douglas Dearth and Alan Campen, *Cyberwar: Myths, Mysteries, and Realities,* AFCEA Press, June 1998; "Eyes Wide Shut," *WIRED Magazine,* August 1997; INTERVIEW "Intelligence Strategique aux Etats-Unis: Mythe ou Realite?" *Revue Francaise de Geoeconomie,* Spring 1997; "Open Sources and Cyberlaw," *Fringeware,* #11, April 1997; "The Military Perspective on Information Warfare: Apocalypse Now," *Enjeux Atlantiques,* #14, February 1997; "Creating a Smart Nation: Information Strategy, Virtual Intelligence, and Information Warfare," in Alan D. Campen, Douglas H. Dearth, and R. Thomas Goodden, contributing editors, *Cyberwar: Security, Strategy, and Conflict in the Information Age,* AFCEA, 1996; "Creating a Smart Nation: Strategy, Policy, Intelligence, and Information," *Government Information Quarterly,* Summer 1996; and "Reinventing Intelligence: The Vision and the Strategy," *International Defense & Technologies,* December 1995, bilingual in French and English; "Private Enterprise Intelligence: Its Potential Contribution to National Security," paper presented to the Canadian Intelligence Community Conference on Intelligence Analysis and Assessment, October 29, 1994. Reprinted in *Intelligence and National Security,* Special Issue, October 1995, and also in a book by the same name, 1996. It merits comment that information is the ultimate asymmetric warfare tool.

33. A few works merit mention here: Vaclav Havel, *Disturbing the Peace: A Conversation with Karel Hvizdala*, Vintage, 1990; Pierre Levy, *Collective Intelligence: Mankind's Emerging World in Cyberspace*, Plenum, 1997; Howard Rheingold, *Smart Mobs: The Next Social Revolution – Transforming Cultures and Communities in the Age of Instant Access*, Perseus, 2002; Tom Atlee, *The Tao of Democracy: Using Co-Intelligence to Create a World That Works for All*, Writer's Collective, 2003; James

Surowiecki, *The Wisdom of the Crowds: Why the Many Are Smarter Than the Few and How Collective Wisdom Shapes Business, Economies, Societies, and Nations*, Doubleday, 2004.

34. Despite repeated efforts from 1992 to 2004 by the author to persuade the Department of State of the urgency of resuming its original responsibility for collecting, processing, translating, interpreting, and disseminating relevant foreign language information of importance to our foreign affairs, culminating in a speech at the State Department on March 24, 2004, "The New Craft of Intelligence: How State Should Lead," co-sponsored by the Secretary of State's Open Forum and the World Affairs Council, at *www.oss.net/extra/news/?module_instance=1&id=2348*, the author was informed by a Deputy Assistant Secretary of State for Intelligence that State desires to be a consumer of intelligence—including open source intelligence—and not a collector of any kind of information, including overt information.

35. SIOP: Single Integrated Operational Plan. When we talk about putting the "I" back into DIME, we are also talking about finally achieving a unified national security and national competitiveness program in which the Planning, Programming, and Budgeting System (PPBS) is applied coherently to diplomatic, information, military, and economic sources of national power, and single integrated DIME campaign plans are executed coherently at the strategic, operational, tactical, and technical levels of performance.

36. Strategic, operational, tactical, technical. The author is indebted to Edward N. Luttwak, whose book *Strategy: The Logic of War and Peace*, Belknap, 1987, not only distinguished among the four levels of warfare, but also showed how capabilities that may be considered deficient at one level actually interact to enable capabilities available at another level—e.g., man-portable antitank guns channeling enemy tanks for artillery, which in turn sets them up for aviation kills.

37. Political-military; socio-economic; ideo-cultural; techno-demographic; natural-geographic. It is not possible to succeed at IO without understanding both the dimensions of revolution and the aspects of socio-psychological personality within a society. Cf. Robert David Steele, *Internal War: A Framework for the Prediction of Revolution*, Lehigh University, 1976. The matrix was first published in Robert David Steele, *On Intelligence: Spies and Secrecy in an Open World*, AFCEA, 2000, p. 153. The matrix is in the Appendix to this monograph.

38. Kristan Wheaton, *The Warning Solution: Intelligent Analysis in the Age of Information Overload*, AFCEA International Press, 2001. Wheaton teaches today at Mercyhurst College, where Robert Heibel, the founder, and Wheaton now are the key figures behind America's first and foremost undergraduate program to teach Intelligence and Research Analysis. See the program at *www.mciis.org/*.

39. Thomas H. Davenport and John C. Beck, *The Attention Economy: Understanding the New Currency of Business*, Cambridge: Harvard, 2001. The elaboration which follows is provided by the author.

40. The Report of the High-level Panel on Threats, Challenges, and Change, *A More Secure World: Our Shared Responsibility*, United Nations, 2004, benefited from

the participation of Lieutenant General (Ret.) Brent Scowcroft, former national security advisor to President George W. Bush. This panel concluded that the greatest threats to global peace and prosperity are, in this order:

- Economic and social threats including poverty, infectious disease, and environmental degradation;
- Interstate conflict;
- Internal conflict, including civil war, genocide, and other large-scale atrocities;
- Nuclear, radiological, chemical, and biological weapons;
- Terrorism; and
- Transnational organized crime.

Hence, terrorism is either fifth on this list or seventh, if the first is counted as three. The report, 262 pp. in length, can be seen at *www.un.org/secureworld/report2.pdf*.

41. The recent announcement of a $100M allocation for a CIA OSINT capability approved by the DNI has been described by some as "a 25-cent raise for FBIS" or "fresh paint for the old lawn chair." In the context of a national intelligence budget of no less than $50 billion a year, $100M is lipstick on the runt pig. Nothing less than a new $3B agency, with a diplomatic or civil affairs character rather than a secret intelligence mandate, will do—half for overseas monitoring, half for bottom-up citizen intelligence processing at the county level across America.

42. Michael Herman, *Intelligence Power in Peace and War*, Cambridge, 1996, points out that most strategic or long-term intelligence is best done using broad access to multilingual open sources, while covert means are best reserved for absolutely vital penetrations of short-term threats not amenable to open source collection. His second book, *Intelligence Services in the Information Age*, 2001, adds additional graduate level reflections to his seminal earlier book. On the American side, the single best book along these lines is by Bruce Berkowitz and Allan Goodman, *Best Truth: Intelligence in the Information Age*, New Haven, CT: Yale, 2000.

43. The greatest deficiency of the existing open source information access capabilities within the U.S. intelligence community, apart from its mind-set and legal and and security obstacles, is its inability to scale globally, address the local, and do complex translations and multisource analysis in near-real-time. A key common finding of several books addressing the challenges of globalization for business is that anything less than global coverage and near-real-time understanding is unsatisfactory. The same literature also advises against "build it first and then try to sell it," instead recommending constant vigilance and instant reaction. Here is a sample quotation:

> Instead of fruitlessly trying to predict the future course of a competitive or market trend, customer behavior, or demand, managers should be trying to find and deploy all the tools that will enable them, in some sense, to be ever-present, ever-vigilant, and ever-ready in the brave

new marketplace in gestation, where information and knowledge are ceaselessly exchanged.

This boils down to global coverage and surge response in combination. Quotation from Regis McKenna, *Real Time: Preparing for the Age of the Never Satisfied Customer*, Harvard, 1997.

44. Ben Gilad, *Business Blindspots: Replacing Myths, Beliefs, and Assumptions with Market Realities*, Tetbury, England: Infonotics, 1996, p. 1, emphasis added. Gilad is also the author of *Early Warning: Using Competitive Intelligence to Anticipate Market Shifts, Control Risk, and Create Powerful Strategies*, American Management Association, 2004, but his earlier work remains his most trenchant—the latter being more about sources and methods.

45. W. Bradford Ashton and Richard A. Klavans, contributing editors, *Keeping Abreast of Science and Technology: Technical Intelligence for Business*, Battelle, 1997, p. viii.

46. *www.academyci.com/About/herring.html*.

47. See, e.g., Craig Fleisher and Babette Bensoussan, *Strategic and Competitive Analysis: Methods and Techniques for Analyzing Business Competition*, Prentice Hall, 2003. As a major on active duty in Sweden, Mats Bjore established the Swedish Long-Range Reconnaissance Unit for Cyberspace, otherwise known as the Swedish Military Open Source Intelligence Centre. He was subsequently nominated by the Royal Academy and received a personal decoration from the King of Sweden for this accomplishment. Together with Detective Steve Edwards in England, the creator of the Scotland Yard OSINT unit who was honored by the Queen of England, Bjore is perhaps the top OSINT performer in the world. He is CEO of InfoSphere AB, *www.inforsphere.se* and also a co-owner of Silobreaker, a UK-based OSINT access portal with tools.

48. Defense Science Board, *Transition to and from Hostilities*, December 2004. Its recommendations are being implemented via DoD Directive 3000.cc dated December 17, 2004, in draft.

49. Numerous military professionals, including the author, have been making the distinction, since the mid-1990s, among the "four forces after next." The annual Army Strategy Conference has consistently brought forth useful contributions, including some iconoclastic ones. The 1998 conference was reported by the author in "The Asymmetric Threat: Listening to the Debate," *Joint Forces Quarterly*, Autumn-Winter 1998-99, at *www.dtic.mil/doctrine/jel/jfq_pubs/1520.pdf*.

50. Foreign Policy in Focus (FPIF), the Center for Defense Information (CDI), and the Security Policy Working Group (SPWG) all generally left-leaning but largely sensible organizations, have come together in an attempt to move money from a heavy metal military toward "soft power" law enforcement and diplomatic or foreign assistance initiatives. See a release leading to the full report at *tinyurl.com/dhjwb*. My personal view is that a Unified National Security Budget is a good idea in theory, but not until the Office of Management restores the management ("M") function. To be effective, a Unified National Security Budget requires (1) a

complete appreciation for all global threats based on access to all open sources in all languages; (2) a national security strategy aware that creating wealth overseas is the fastest way of stabilizing very large populations; and (3) a Vice President or a Secretary-General for National Security that has command and control over State, Justice, and Defense, together. Right now State does not want to lead, Justice is incapable of leading, and Defense is too busy to lead an interagency program.

51. The UN Report, *supra* note 39, points out that biological security is a major concern.

52. The definitive work on why supporting 44 dictators makes our global stabilization program impossible to achieve is that of Ambassador Mark Palmer, *Breaking the Real Axis of Evil: How to Oust the World's Last Dictators by 2025*, Lanham, MD: Rowman & Littlefield, 2003. Ambassador Palmer recommends an Undersecretary for Democracy with two Assistant Secretaries: one for the dictators that agree to a 5-year buy-out, and one for the ones that do not. We would add our own complementary recommendation: an Undersecretary of Defense for Peacekeeping, with two Assistant Secretaries: one for the failed states that agree to accept our help, and one for the ones that do not.

53. Dictators itemized in Mark Palmer, *Breaking the Real Axis of Evil;* plagues from *State of the World Atlas*, 1997; water scarcity discussed by Marq de Villiers, *Water: The Fate of Our Most Precious Resource*, Mariner, 2001; resource wars in Michael Klare, *Resource Wars: The New Landscape of Global Conflict*, Owl, 2002; all others from the *Map of World Conflict & Human Rights*, PIOOM, 2002.

54. Cf. Jonathan Schell, *Unconquerable World: Power, Non-Violence, and the Will of the People,* Owl, 2004.

55. This is a point made by Dietrich Bonhoeffer and captured in a DVD under his name.

56. Max Manwaring, contributing editor, *The Search for Security: A U.S. Grand Strategy for the Twenty-First Century*, Westport, CT: Praeger, 2003. See also Max Manwaring, contributing editor, *Environmental Security and Global Stability: Problems and Responses*, Lexington, KY: Lexington, 2002; Max Manwaring and Anthony James Joes, contributing editors, *Beyond Declaring Victory and Coming Home: The Challenges of Peace and Stability Operations*, Westport, CT: Praeger, 2000; Max Manwaring and John Fishel, contributing editors, *Toward Responsibility in the New World Disorder: Challenges and Lessons of Peace Operations*, London: Frank Cass, 1998.

57. On the negative effects of corruption and immoral capitalism, see, for instance, John Perkins, *Confessions of an Economic Hit Man*, San Francisco: Berrett-Kohler, 2004; and William Greider, *The Soul of Capitalism: Opening Paths to a Moral Economy*, New York: Simon & Schuster, 2003. On the need to nurture three billion new capitalists and to have a strategy for energy independence, among other key protective measures, see Clyde Prestowitz, *Three Billion New Capitalists: The Great Shift of Wealth and Power to the East*, New York: Basic Books, 2005. Within the United States, there are numerous books on the manner in which the national security

policy process is corrupted by special interests, including foreign interests. In combination, ground truth and morality are the two greatest weapons in America's arsenal. They are rusty and unused weapons. Putting the I back into DIME will make them shiny, bright, and useful again.

58. The DoD overview document signed by Deputy Secretary of Defense Gordon England is *Strategy for Homeland Defense and Civil Support*, Washington, DC: Department of Defense, June 2005, at *www.defenselink.mil/news/Jun2005/d20050630homeland.pdf*.

59. The existing Open Source Information System (OSIS) is very well-managed within the legal and security constraints imposed by industrial-era intelligence mind-sets. It is incapable of rising to the challenge of global open source information sharing across both DHS and NGO boundaries. Only a commercial implementation will meet this need. It merits comment that FedEx is approved for the transmission of SECRET documents. OSIS-X will easily qualify for at least SECRET and probably TOP SECRET when using commercial encryption, audit trails and receipts, and by-name access controls. We respectfully note here that no official connection is implied between OSIS (created and managed by the government) and OSIS-X (to be created and managed by the private sector). We have chosen to use OSIS-X as a "shorthand" name because of the very broad appreciation, both within the United States and overseas, of the concepts and protocols established by OSIS under Intelink leadership. We also believe, as illustrated in our pyramid, that Intelink-X is inevitable and essential if we are to achieve true multinational, multiagency, multidisciplinary, and multidomain information-sharing at multiple levels of classification. Multilateral sharing, not bilateral sharing, will be the key characteristic of government intelligence as well as private sector intelligence in the 21st century.

60. All vendors, without preference, will have no alternative but to rapidly adopt and offer to their clients CISCO's AON, the latest advancement in secure controlled routing technology. AON is specifically targeted to customers whose applications have proliferated into siloed and fragmented environments and who must now integrate these applications and services to improve collaborative business processes. AON is the first and only network-embedded intelligent message routing system providing ubiquitous, adaptable message-level communication, visibility, and security. These enable applications and the network to work together as an integrated system without requiring new intermediary layers or changes to existing applications. Also, this can be delivered in a network-based solution that is pervasive throughout the IT infrastructure. Today it is available to federal clients from L-3 Communications, MANTECH, and SAIC.

61. This can be as simple as a cell phone with an open source browser that includes a known return address and password sequence for authenticating the individual's access.

62. Congressman Robert Simmons (R-CT-02) is a member of the House Armed Services Committee and also of the committee responsible for Homeland Security. He is the "owner" of OSINT issues within the House, having championed OSINT

before it became fashionable. His most recent hearing focused exclusively on OSINT in support of homeland defense. We anticipate a strong Congressional interest in how DoD and DHS can collaborate in making global OSINT, and domestic OSINT, more readily useful to the defense of our citizens here at home.

63. DHS has First Source and EAGLE acquisition projects. OMB has several task forces seeking "common solutions" for the entire federal community. The IC has its own solutions, including an unworkable expansion of OSIS out to the state and local authorities. DoD has its USDI investments. GSA has a collaborative tools network. DARPA has its own diverse investments, as does NASA, NOAA, and so on. Nowhere in the U.S. Government does there appear to be a focus on the urgency of creating a truly national information-sharing system that is built on a foundation of affordable open source software, shareable open source information, and accessible open (electromagnetic) spectrum.

64. Executive Order 12333 long has demanded the presumption that anyone within the United States should be presumed to be a U.S. citizen when inadvertently captured via classified collection means, but this does not apply to open sources and methods. One is also allowed to collect freely on individuals in the United States when they are known to be in association with a foreign power or thought to be an agent of a foreign or terrorist organization considered a threat to national security.

65. Cf. David Born and Edward Perkins, contributing editors, *Preparing America's Foreign Policy for the 21st Century*, Norman: University of Oklahoma, 1999.

66. Thomas L. Friedman, The *World is Flat: A Brief History of the Twenty-First Century*, New York: Farrar, Straus, and Giroux, 2005.

67. Henry Kissinger, *Does America Need a Foreign Policy? Toward a Diplomacy for the 21st Century*, New York: Simon & Schuster, 2002. From the author's Amazon.com review of this book: The core point in this entire work is that both economics and technologies, including Internet and communications technologies, have so out-paced politics that the world is at risk. Globalization, terrorism, and other threats cannot be addressed with our existing international, regional, and national political constructs, and new means must be found—new political solutions must be found—if we are to foster security and prosperity in the age of complexity, discontinuity, and fragmentation.

68. Alvin and Heidi Toffler are publishing a new book in April 2006 tentatively titled *Revolutionary Wealth*. It will surely build on their quarter century of informed observation and reporting, as well as the works of others, such as Thomas Stewart's *The Wealth of Knowledge* and Barry Carter's *Infinite Wealth*, *supra* note 3. In the technical arena, the two most recent books covering genetics, robotics, and nanotechnology are those of Joel Garreau, *Radical Evolution*, New York: Doubleday, 2005; and Ray Kurzweil, *The Singularity is Near*, New York: Viking, 2005.

69. This was the major finding of the National Imagery and Mapping Agency Commission Report of December 1999, concluding that we have been spending

tens of billions of dollars on esoteric collection systems, without a commensurate investment in information technologies for Tasking, Processing, Exploitation, and Dissemination (TPED). Even today, as the IC experiments with ICMAP reveal, OSINT, though intended to be an all-source collection management tool, is not represented and the tool fails to provide for establishing whether we already know the information, whether an ally knows the information, or whether we can obtain or buy the information from the private sector.

70. *Defense Science Board 2004 Summer Study on Transitions to and from Hostilities*, Washington, DC: Undersecretary of Defense for Acquisition, Technology, and Logistics, December 2004.

71. *Ibid*.

72. *Report to the President of the United States*, Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, Washington, DC, 2005.

73. *The National Strategy for Homeland Security*, The White House, 2004.

74. *Information-sharing for Homeland Security: A Brief Overview*, CRS, January 10, 2005.

75. *Supra* note 9.

76. Multinational, multiagency, multidisciplinary, multidomain information-sharing.

77. The trolleys rolled into Congress with boxes and boxes of documents associated with the hearings for the nomination of Judge Roberts to the Supreme Court could be considered by a skeptic to be a sign of the administration's desire to make it difficult for Congress to process the information. The reality is that across the federal government, hard-copy industrial era processes that are labor-intensive still rule. Interns screen the mail to a Cabinet secretary, and, more often than we'd suspect, information coming into an agency is lost before it ever reaches the right person.

78. A concluding recommendation suggests that there is a need for a Combatant Commander for Intelligence and Information Operations (I2O), and that if such a COCOM is created, STRATCOM should be redirected to focus on planning and managing Big War. A case could also be made for a new COCOM for S&R, or it could be assigned to SOCOM or NORTHCOM, depending on the prevailing view within DoD leadership as to whether S&R is more closely related to containing terrorism or helping failed states recover from disaster in all its forms.

79. Code M320 was created by Sean O'Keefe, Deputy Director of OMB at the time (2000-01), acting on the advice of Don Gessaman, former Associate Deputy Director of OMB for National Security, who was, in turn, informed by the author.

80. One such expert, perhaps the ideal expert to help DoD and DHS work together, is Michael C. Daconta, author and co-author of 10 technical books, Chief Architect of DIA's Virtual Knowledge Base, inventor of Fannie Mae's Electronic

Mortgage Standard, and today the DHS Metadata Program Manager with responsibility for being the lead for the FEA DRM Working Group, and the co-lead for NIEM.

81. In general the aggregators, whose value was undeniable years ago, are no longer worth the price of their demanded "gold license." They still tend to be largely a collection of English-language sources focused on business. Where they offer historical or cultural information this tends to be deceptive—token coverage rather than comprehensive. The cost, price, and technology model of the traditional aggregators are no longer competitive.

82. California is in the process of adding 20 analysts and an open source information collection and exploitation capability to its statewide intelligence network. We believe that every state will benefit from the USDI initiatives in the future.

83. This recommendation is consistent with the Defense Science Board report *Strategic Communication,* July 2004; and with *Transitions to and from Hostilities*, December 2004. However, by deliberately funding open source software collaborative work tools that can allow NGOs and state and local authorities to join the larger DoD network, the information power of these regional centers will be considerably enhanced.

84. Googling for DARPA STRONG ANGEL will produce various references. A roster of key players is provided by Commander Eric Rasmussen, USN, who is the driving force, at *www.baselinemag.com/article2/0,1540,1813578,00.asp*. The other key person is Dave Warner of MindTel.

85. USSOCOM has $2M earmarked in 2006 for hand-held tactical computers. Separately, the World Bank is funding millions of Motorola cell phones that will be given out across the Third World to energize micro-capitalism. Somewhere between these two initiatives is the next hand-held that will be the sole communications and computing device for the billions of individuals in the Third World. Hence, it must be interoperable with OSIS-X.

86. Two excellent reports that illuminate the problems that persist are *Defense Acquisitions: The Global Information Grid and Challenges Facing Its Implementation*, Washington, DC: U.S. Government Accountability Office (GAO), July 2004; and *Information Technology: Major Federal Networks that Support Homeland Security Functions*, Washington, DC: GAO, September 2004. In both reports, GAO makes it clear that what we have now is not working, and what we have planned is out of date.

87. Although the DOSC lacks representation from policy offices, operational commanders, acquisition managers, and logisticians, it nevertheless fulfilled its mandate from USDI.

88. The author is an elected member and was present for this discussion.

89. As recorded in Robert David Steele, *On Intelligence: Spies and Secrecy in an Open World*, AFCEA, 2000, p. 36. The GDIP account is based on personal recollection. Mr. Marty Hurowitz and Mr. Keith Hall were parties to the conversation.

90. Colonel Pheneger received a Golden Candle Award in 1995.

91. An excellent world map depicting the current 16 missions and the manpower involved (over 60,000 personnel) is at *www.un.org/Depts/dpko/dpko/bnote.htm*.

92. NASA has been experimenting with XML-Geo. There are undoubtedly other standards under consideration. Establishing a geospatial tagging standard must be a high priority if we are to reap the benefits in 2006 and beyond.

93. The first is from IcoSystem, a pioneer in visualization; the second from Dr. Dave Warner of MindTel, a pioneer in creating TIDES and other means of predictive analysis.

94. Which would include the CISCO AONS and the geospatially-compliant data meta-tagging that Team L-3 provides.

95. Apart from its relative lack of concern about security (with constant patches being the norm), as opposed to Macintosh or Linux, Microsoft now brags that most of its code is being written in China and India, both of whom have every opportunity to plant back doors and Trojan Horses into software being delivered to Microsoft for mass marketing.

96. This capability can be examined at *www.silobreaker.com*. It is the heart of the OSS.Net system for producing multi-lingual OSINT.

97. This is not the Federally-Funded Research and Development Center (FFRDC) envisioned by the Director of National Intelligence (DNI) and his staff. Any FFRDC that is beholden to and subordinate to the legal, security, and mind-set biases of the U.S. intelligence community is "dead on arrival." Instead, this is envisioned as similar to the Microelectronics and Computer Technology Corporation (MCC), a unique private partnership created to help the United States preserve its edge in computer technology and led for a time by Admiral Bobby Inman, USN, Ret. With an antitrust waiver from the Department of Commerce, this skunk works would focus on creating public intelligence sources, softwares, and services that elevate the utility of all information to all citizens all the time.

98. Peter G. Peterson, *Running on Empty: How the Democratic and Republican Parties Are Bankrupting Our Future and What Americans Can Do About It*, New York: Picador, 2005. The author is remarkable for being President of the Council on Foreign Relations and therefore very much an "establishment" personality.

99. Cf. Jonathan Schell, *The Unconquerable World: Power, Nonviolence, and the Will of the People*, Metropolitan, 2003.

ABOUT THE AUTHOR

ROBERT DAVID STEELE, having sponsored an annual international conference on Open Source Intelligence (OSINT) and what the Swedes call M4 IS, or multinational, multiagency, multidisciplinary, multidomain information-sharing, is a leading proponent for these activities. As the senior civilian founder of the Marine Corps Intelligence Command (1988-92) and subsequently as CEO of OSS. Net, Inc., he has spent 17 years in advocacy. A former clandestine case officer with the Central Intelligence Agency (CIA), he has served three back-to-back clandestine tours overseas, participated in strategic signals acquisition operations, helped program future imagery satellites, managed a global counterintelligence program against a denied area country, and defined future advanced information and processing requirements for a national agency. It was as the senior civilian at the Marine Corps Intelligence Command that he discovered that 80 percent of the information needed to do policy, operational, logistics, acquisition, and all-source intelligence was not secret, not in English, not online, and not visible to anyone in the National Capital Area (NCA). Prior to becoming a civilian intelligence professional, first at the CIA and then as a manager for the Marine Corps, he served as an infantry officer. Mr. Steele is the author of *On Intelligence: Spies and Secrecy in an Open World* (AFCEA, 2000) and *The New Craft of Intelligence: Personal, Public, and Political* (OSS, 2002). He is a contributing editor of *Peacekeeping Intelligence: Emerging Concepts for the Future* (OSS, 2003) and *Peacekeeping Intelligence: The Way Ahead* (forthcoming). He has been featured in the *Year in Computers 2000* and twice recognized by *Microtimes* as one of the "industry leaders and unsung heroes who…helped create the future." He is featured in the chapter on "The Future of the Spy" in Alvin and Heidi Toffler's *War and Anti-War: Survival at the Dawn of the 21st Century*, where they discuss OSINT as "the rival store." Mr. Steele holds an AB in Political Science from Muhlenberg College, an MA in International Relations from Lehigh University, and an MPA in Public Administration from the University of Oklahoma. He is a distinguished graduate of the Naval War College, and received a certificate in Intelligence Policy from Harvard University.