THE NEW CRAFT OF INTELLIGENCE: ACHIEVING ASYMMETRIC ADVANTAGE IN THE FACE OF NONTRADITIONAL THREATS

Robert D. Steele

February 2002

*****

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. Copies of this report may be obtained from the Publications Office by calling commercial (717) 245-4133, FAX (717) 245-3820, or via the Internet at Rita.Rummel@carlisle.army.mil

*****

Most 1993, 1994, and all later Strategic Studies Institute (SSI) monographs are available on the SSI Homepage for electronic dissemination. SSI's Homepage address is: http://www.carlisle.army.mil/usassi/welcome.htm

*****

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 let us know by e-mail at outreach@carlisle.army.mil or by calling (717) 245-3133.

ISBN 1-58487-083-4

FOREWORD

Since the mid-1990s, the concept of strategic asymmetry has been receiving more serious attention from the U.S. Department of Defense. The September 11, 2001, attack on America, in which fully-loaded airplanes used as a form of stealth bomb with aerial fuel explosives hit the World Trade Center and the Pentagon, marked the beginning of an actual asymmetric war. Its initial dimensions shocked and engaged the Nation.

This monograph, by Robert D. Steele, is the third in the Strategic Studies Institute's "Studies in Asymmetry" Series. In it, the author examines two paradigm shifts—one in relation to the threat and a second in relation to intelligence methods. He offers new models for threat analysis and for intelligence operations in support of policy, acquisition, and command of forces engaged in non-traditional asymmetric warfare. He concludes with an examination of the Revolution in Military Affairs and the need for a Revolution in Intelligence Affairs.

DOUGLAS C. LOVELACE, JR.
Director
Strategic Studies Institute

BIOGRAPHICAL SKETCH OF THE AUTHOR

ROBERT D. STEELE is a retired Marine Corps infantry and intelligence officer. He is the founder and president of Open Source Solutions, Inc., and is an acknowledged expert on computer and information vulnerabilities. Mr. Steele holds graduate degrees in International Relations and Public Administration from Leigh University and the University of Oklahoma. He has also earned certificates in Intelligence Policy from Harvard University and in Defense Studies from the Naval War College.

SUMMARY

Both the Cold War threat paradigm and the Cold War intelligence paradigm are dead. A new integrative paradigm for achieving asymmetric advantage in the face of nontraditional threats is needed in the face of both nontraditional threats and nontraditional sources and methods. This can be done by devising and exploiting new intelligence sources and methods.

The **old threat paradigm** emphasized strategic nuclear and conventional forces associated with a government, with static orders of battle, linear in development and deployment over time. They were employed in accordance with well-understood rules of engagement and doctrine, were relatively easy to detect in mobilization, and were supported by generally recognizable intelligence assets.

The **new threat paradigm**, in contrast, is generally nongovernmental (or a failed state), nonconventional, dynamic or random and nonlinear in its emergence, with no constraints or rules of engagement. It has no known doctrine, is almost impossible to predict in advance, and is supported by an unlimited 5th column of criminals, terrorists, drug traffickers, drug addicts, and corrupt individuals. It is, in a word, asymmetric.

The **old intelligence paradigm** relied heavily on secret and very expensive technical collection against one main target, the Soviet Union. Such information-sharing relationships as existed within the national and military intelligence communities have been both secret and on a bilateral basis.

The **new intelligence paradigm** must embrace and cope with the information explosion, and especially the explosion in multilingual digital information, while also

managing to obtain truth on the ground from every clime and place through direct observation by trained Army Foreign Area Officers (FAO).

This **new craft of intelligence** requires that four quadrants of knowledge be fully developed, in an integrated fashion. Only one of these quadrants is secret. The first exploits the lessons of history; the second develops web-based means of sharing the burden of achieving global coverage; the third harnesses the full distributed intelligence capabilities of the entire Nation; and the fourth utilizes spies and secrecy to great effect.

With the new craft of intelligence well in hand, with a new strategy that understands the continuum of personnel skills needed from homeland defense to overseas power projection, the Army may be ready to consider radical changes in how it recruits, trains, equips, and organizes the active, reserve, and National Guard forces. If we have entered a period of total war, with no front lines, it may be that the Army should devise a new "total force" concept for asymmetric operations on the homefront and overseas.

The monograph recommends several initiatives for Army leadership. They are: establishment of a homeland defense intelligence program, including a homeland defense analysis center and community intelligence centers in each state or commonwealth; a digital history and captured document project and processing center; and four major regional open source activities responsive to both the theater commanders and general national security needs. Additional initiatives include a web-based global information-sharing consortium to reduce the cost and time associated with global coverage activities of threats of common concern, and especially nontraditional asymmetric threats; and, close collaboration with Joint Forces Command to create a generic analytic workstation and a generic open source intelligence training program suitable for homeland and overseas partners.

THE NEW CRAFT OF INTELLIGENCE: ACHIEVING ASYMMETRIC ADVANTAGE IN THE FACE OF NONTRADITIONAL THREATS

INTRODUCTION

The attack of September 11, 2001, has brought to the fore the importance of strategic *balance* or *diversification*. We must have balance between our homeland defense and overseas defense capabilities; between domestic counterintelligence and foreign intelligence; and between symmetric and asymmetric concepts and doctrine and forces. In this monograph, the author reviews the global nontraditional threat situation, briefly updates the prospects for intelligence reform, and then lays out the details for the new craft of intelligence—a craft that is comprehensive, reliable, swift, and *relevant* to both the immediate and the longer-term threats.[1] The new craft of intelligence must be held accountable for explaining the threat in such compelling terms that political action cannot be denied—one means of doing so is by issuing public intelligence estimates and public intelligence warnings.

None of the traditional threats that our military understands have diminished—indeed, the attacks of September 11 demonstrate that our world is perhaps twice as dangerous as we might have imagined. America is very much "on its own," and whatever new craft of intelligence it may adopt, we must be able to achieve an asymmetric advantage over every threat to our national security and our national prosperity. Intelligence is vital to our future security, not only overseas but at home where we need a new craft of *counter*-intelligence.[2] The new craft of intelligence must overcome both the political and the professional shortcomings that have plagued U.S. intelligence and counterintelligence for over a half-century. The U.S. Army,

the U.S. Army Reserve, and the National Guard can and should lead the way, at home and overseas.

Strategy must precede force structure and weapons programs, and a good appreciation of the threat must precede the formulation of strategy. We must get intelligence right if all else is to follow. In the aftermath of the September 11 attack, we now realize that, in combination, our intelligence deficiencies and our lack of concepts, doctrine, or force structure for homeland defense left us terribly vulnerable to attacks that are asymmetric in targets, means, execution, and context.[3] The September 11 targets, all within the homeland, were both symbolic and undefended. In the first great battle of the asymmetric era, surprise was total and the losses catastrophic.

The choice of means was brilliant in its daring and conceptualization—low-cost, high-concept asymmetry. For the price of 19 airline tickets and a year's preparatory expenses, four fully-loaded transcontinental domestic airline vehicles were turned into precision munitions, delivering huge aerial fuel explosives with catastrophic results in New York and startlingly severe results in Washington, DC. Only the heroism of the passengers on the fourth flight—each now empowered by foreknowledge of their future fate—saved another building, perhaps the U.S. Capitol. The prompt action of the Federal Aviation Administration in grounding the fleet may have prevented other hijackings. The means were brilliant in acquisition and result, but also in stealth. This was, in effect, the Trojan Horse of the 21st century, only it was a Trojan Horse built by our own companies that could be flown directly into the most attractive targets, without opposition and to great effect. Henceforth, "the threat" must be considered in the context of an America vulnerable to asymmetric attack "behind the lines"—within our borders. The time has come for intelligence to step back, reconstruct itself, and emerge into the 21st century as the foundation for a new strategy and a new force structure.

The U.S. Army—and the special relationship that exists among the regular Army, the Reserves, the National Guard, and the employers of America—could become the institutional backbone of a new networked "total force" that includes citizens (the "minutemen"), corporations, state and local law enforcement, and other authorities (e.g., public health), as well as national agencies and international elements. The U.S. Army is the one institution capable of an end-to-end paradigm shift that could impact on both domestic and overseas security. If the new craft of intelligence as articulated in this monograph meets with approval within the U.S. Army, it could readily be migrated to the new Homeland Defense Agency, state and local authorities, and to all elements of the national security community, both those in uniform and those in the civilian sector.[4]

The External Threat.

In the year 2000, 26 severe conflicts took place between states, 78 less severe but persistent conflicts between states, and 178 violent *internal* political and ethnic conflicts. In addition to this plethora of under-reported and little understood real-world, right-now conflicts, our security and our prosperity in the 21st century are threatened by a combination of water scarcity, failed states, ethnic fault lines between nations that do not exist and states that do, and opportunistic thugs thriving under conditions of chaos.

Globalization and localization are two sides of the same coin—what happens in Africa, or along the Slavic-Islamic and Sino-Slavic borders (where water scarcity and ethnic confrontation coincide) really matters to mainstream America because "the water's edge" is no longer an effective barrier against weapons of mass destruction; epidemic disease; mass migrations; and virulent electronic vandalism, theft, and terrorism.[5] These nontraditional threats are directly related to the terrorist attack of September 11 because the billions of dispossessed,

disheartened people see in American consumerism and American disengagement a threat to their own well-being.[6] Within this global environment of instability and despair, terrorists hide and multiply.[7]

Home Front Vulnerability.

However catastrophic, however outrageous, however much we may wish to call this an act of war (thereby glorifying and elevating the terrorists that carried out this act), we must avoid the temptation to militarize our response lest we militarize America. The best advice to the President in this time of terror is "revitalize intelligence; understand the threat; restructure the force." Only then will we be ready for the long campaign of joint intelligence, diplomatic, economic, law enforcement, and covert and overt military actions that are called for if we are to stabilize the world and prevent many more attacks—both from terrorists and copycats—around the world.

The whole point of terrorism is to evoke such reactions as might be helpful to the terrorists in recruiting others or inspiring others. Now that we realize numerous terrorists are willing to die, it would seem sensible, before we execute any foreign military or other actions, to first review our home front vulnerability. The new craft of intelligence must provide for *domestic* intelligence and net assessments such as have never been contemplated before. It is no longer possible to discuss intelligence without carefully considering both asymmetric threats and home front defense needs. The U.S. Army and the National Guard are ideally suited to carry out home defense against all manner of threats.[8]

Intelligence-Based Strategy.

The half-way point, the bridge between understanding the threat and structuring the force, lies in the formulation and validation of a national grand strategy that clearly specifies our long-term security objectives, our plans for

achieving those objectives, the capabilities needed for fulfilling our plans, and the steps that we must take in the near- and mid-term to create and maintain those capabilities. At least half of what we must do will be defensive, but not military, in character—we must in some ways militarize how we manage "soft power."[9] Intelligence is the vital underpinning for strategic policy, strategic acquisition, and strategic operational decisions.

PART I—THE THREAT

Professor Martin Van Creveld has observed on more than one occasion that the war colleges of today begin their study of war with the wrong period—the period of the *levee en mass*—the structured armies of Frederick the Great; what some might call the first representation of the traditional state-on-state or force-on-force "traditional threat."[10] Van Creveld suggests instead that we all should begin our study of war with the Middle Ages and gang warfare—what many consider to be the "nontraditional threat." There is much to what he says—indeed, he was a decade ahead of the rest of us in this observation. As the brief review of selected works below will show, a growing body of literature suggests that modern conflict is anything but organized and often not about conventional force-on-force operations. On September 11, 2001, the nontraditional threat shocked the entire world out of its complacency. Every world leader and every person with access to a television was confronted with the power and ambiguity of asymmetric warfare.

Today ethno-nationalist conflicts (state versus nation) are almost half the problem, with inter-ethnic or tribal conflicts and anti-regime wars (state versus insurrection) comprising another quarter. State versus state are just over 10 percent of the types, with decolonization wars, gang wars, and genocide comprising the balance of the last quarter. This is where professional military officers and their civilian policy counterparts will find a strategic view of the global battlefield, clearly identifying 29 countries with

declared emergencies by the United Nations (U.N.); 67 countries with millions of refugees and displaced persons between them; and 27 countries with severe food scarcity and all that implies in terms of death, disease, and crime. There are 42 countries with child soldiers killing one another, 62 countries with unmarked fields of landmines, 94 countries where torture is a common practice, 78 countries where corruption is the norm, and the many countries where censorship is very high.[11] State vs. state conflict is but 10 percent of the real-world conflict.

In this context, peace operations are the dominant form of military activity. They require at least as much forethought, commitment, and sustainment as combat operations. Food scarcity and dangerous public health are the root symptoms, not the core issues. The most dangerous element is not the competing sides, but the criminal gangs that emerge to "stoke the fires of nationalism and ethnicity in order to create an environment of fear and vulnerability" (and great profit). At the same time, humanitarianism has become a big part of the problem—we have not yet learned how to distinguish between those conflicts where intervention is warranted (e.g., massive genocide campaigns) and those where internal conflicts need to be settled internally. In feeding the competing parties, we are both prolonging the conflict, and giving rise to criminal organizations that learn to leverage both the on-going conflict and the incoming relief supplies.

For the professional military officer, several facts are important: (1) no international intelligence system in place is suitable to providing both the global coverage and public education needed to mobilize and sustain multinational peacekeeping coalitions; (2) the U.N. is not structured, funded, nor capable of carrying out disciplined effective peacekeeping operations, and the contributing nations are unreliable in how and when they will provide incremental assistance; and (3) we still have a long way to go in devising new concepts, doctrines, and technologies and programs for effectively integrating and applying preventive diplomacy,

transformed defense, transnational law enforcement, and public services (water, food, health, and education) in a manner that furthers regionally-based peace and prosperity instead of feeding the fires of local unrest. Perhaps of greatest concern, however, is that our own existing intelligence system is not effective against these kinds of threats and these kinds of instability factors.

The Grand Chessboard.

It is helpful to place the pestilence and instability of Africa in a larger geostrategic context. That is clearly one area that must be of concern to our strategists. There are three others. First is Eurasia, rich in energy resources while also facing major ethnic and water scarcity standards, and surrounded by France and Germany to the west, Russia to the north, China to the east, and Turkey and Iran to the south. Second is the Asian archipelago, running from Korea to Taiwan to Indonesia via the Philippines, with China running down two-thirds of the archipelago, Vietnam in the middle, and Australia to the south. The last "flashpoint" region is India and Pakistan, together with the instabilities of Bangladesh and Myanmar to the west, Afghanistan to the north, and Sri Lanka to the south. A common theme in each of these areas is the clash of religions—Muslims and all others—in a context of ethnic conflict, disconnects between tribal nations that have no land and the states that claim the land, and severe water scarcity—especially along the border regions between Russia and China and between Russia and the Islamic lands running along its southern frontier. Figure 1 shows a depiction of these areas, with some key characteristics.[12]

North America, Russia, and Australia are not replenishing their populations. North America, Europe, and Russia are under severe immigration pressure. On the positive side, North America, Russia, and Australia are very rich in resources—head and shoulders above the rest of the world.

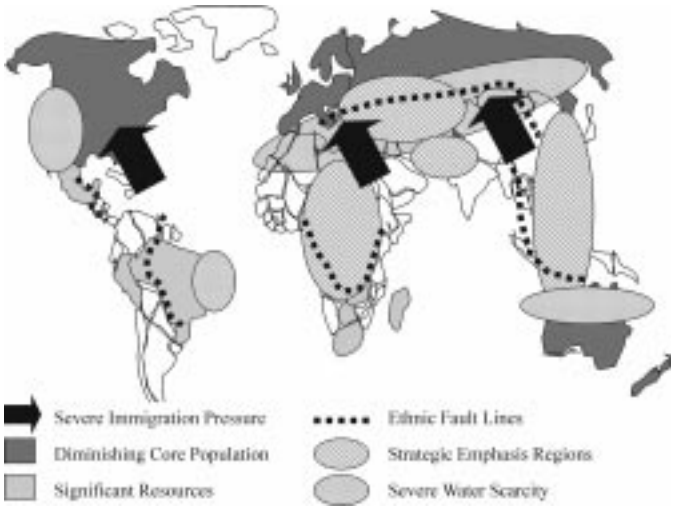

Figure 1. Nontraditional Threat Overlay.[13]

The nontraditional threat appears to be best understood as a race between sustainable development on the one hand, and a spasmodic and very destabilizing population explosion. North America, Europe, and Russia must either find a way to stabilize and contain that population explosion, or they face the real possibility of being "over-run" by dispossessed masses of humanity capable of bringing down any state. The new craft of intelligence is proposed as the primary means for achieving an asymmetric advantage in dealing with the nontraditional threat over time. This point merits further emphasis, for the new craft of intelligence must be capable of putting this race—this threat to our future—in a context that compels understanding and action among citizens, corporations, and governments.

Threat Typology.

The U.S. military has focused on traditional state enemies and the strategic nuclear-conventional threat represented by nation-states. It took an act of Congress to create the Special Operations Command and the related Special Operations and Low Intensity Conflict (SOLIC)

earmarked program. Although the fall of the Berlin Wall inspired many to speak and write of a "peace dividend," and to enthuse over how a Revolution in Military Affairs (RMA) could be funded by this peace dividend, the reality has been disappointing. In combination, the heavy commitment of forces worldwide and a very high tempo of operations have prevented the U.S. military from seriously considering nontraditional threats.

In the current strategic environment, there are four distinct types of threats. Each represents a different challenge requiring a different "way of war" and consequently different concepts, doctrine, and force structure as well as a different approach to intelligence.

High-Tech Brutes—the Violent State Threat.[14] This warrior class relies on strategic nuclear and conventional capabilities, including uniformed troops and marked equipment. It applies high-technology to achieve some physical stealth and relies heavily on precision targeting. The primary threat that we focused on during the Cold War is the threat that we understand best. Russia, China, North Korea, Iraq, India, Pakistan, and, to a much lesser extent, Cuba, represent this kind of threat. The major countries in Europe, were they to become our enemy, represent this kind of threat. This is also the *easiest* threat to monitor and the easiest threat to plan against because it is so obvious, so large, and so complex that it cannot, by and large, surprise us.

Low-Tech Brutes—the Violent Nonstate Threat. The "low-tech brute" is violent but generally does not represent a state. Terrorists and transnational criminal gangs present both defense and intelligence with the "low slow singleton threat" that is extremely difficult to detect in the absence of a pervasive human intelligence network. This threat is also very "random" in nature in that it does not have obvious military goals and can rely on an unlimited fifth column of either well-paid volunteers, or volunteers recruited for one-time *in extremis* support tasks.

The low-tech brute is the most common threat to the good order and prosperity of organized states and their peoples. Unlike "low-intensity conflict" threats for which Congress wisely created the Special Operations Command and the SOLIC Program, the low-tech brute is not necessarily "organized" into a revolutionary army but rather is an aggregation of violent individuals who come together in random or covert ways that are extraordinarily difficult for our intelligence and law enforcement communities to detect and counter. Terrorism, and especially radical faith-based terrorism, is the ultimate manifestation of this kind of threat, and also unusual because it prefers to fight within the U.S. homeland rather than overseas.

Our national security structure—in policymaking terms, in acquisition terms, and in day-to-day operational capability terms—is not geared to challenge this threat class effectively.[15] As the September 11 attack demonstrated so clearly, we do not have integrated national intelligence watch lists and communications; we do not have a national homeland defense analysis or counterintelligence capability in place; and we have not put in place fully effective measures against internal attacks.

Low-Tech Seers—the Nonviolent Nonstate Threat. This "threat" class is not inherently violent but is characterized by the unresolved and largely legitimate needs of large groups of people whose circumstances, culture, and history force them into confrontations with either established states or other nonstate groups. At root is the quest for water, food, and freedom from fear. However, this threat class should also be viewed as the "sea" within which terrorists may swim undetected. Among the greatest homefront challenges facing America is that of discerning between loyal immigrant citizens and disloyal dangerous immigrant terrorists who mean to do great harm. The lack of trained law enforcement personnel from our diverse cultural base and of translators for all of the major languages for this threat group should be of great concern.

Our intelligence community and national security policymakers have neglected this threat because it has been perceived as one that does not require the collection of secrets and one that can be adequately understood through common academic, think tank, business, and other nongovernmental study.[16] In fact, because this threat class numbers billions of human beings, it may ultimately be the most serious.

High-Tech Seers—the Volatile Mixed Threat. In just the past few years, a new threat has catapulted itself to the top position in our consciousness. Although terms such as cyberwar and information warfare are in vogue, this threat is much more complex. On the one hand, we see in this threat class, deliberate state-sponsored capabilities to wreak havoc with our domestic infrastructure (power, communications, transportation, and finance) as well as individual or gang capabilities to be very destructive while remaining anonymous. On the other, we see more subtle uses of electronic access to conduct economic espionage at the state level, "political theft" at the terrorist gang level, and plain theft at the individual level. This threat class also includes information vandalism by our own disgruntled citizens as well as outsiders and corporate irresponsibility in failing to provide properly developed communications and computing products that are "safe" on the information superhighway.[17] Finally, this threat class can combine with any other class, for instance with the low-tech brutes, to create a hybrid threat.

Threat Typology.

Figure 2 illustrates these four threat types, with some additional information on the different kinds of war they might engage in, as well as their sources of strength, their preferred mode of stealth, and their normal targeting practice.

We now know, in the aftermath of the September 11 attack, that we seriously underestimated the strategic

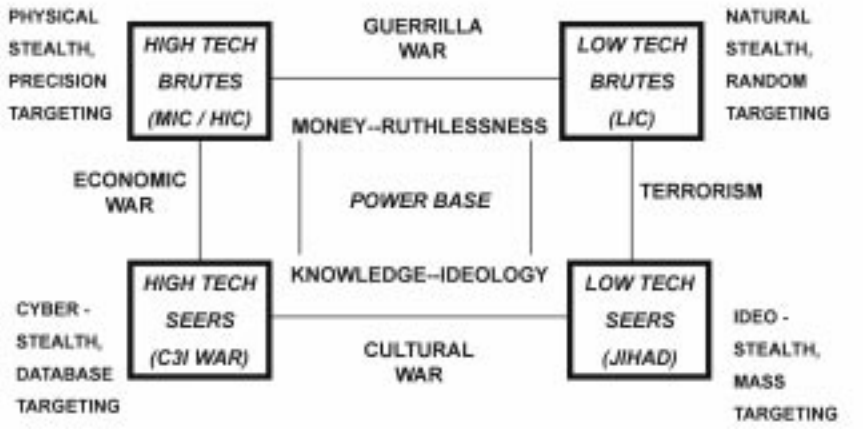

Figure 2. Four Threat Types.

brilliance, the financial self-sufficiency, and the obsession with confronting America on its home ground, of one man: Osama bin Laden. Causing over 4,000 casualties—almost all deaths—in one day, more than we ever suffered during our long confrontation with the Soviet Union and several times the casualties of Pearl Harbor, his directed actions have defined the beginning of a new period of danger, the beginning of the age of asymmetric warfare. Both our foreign intelligence and our domestic counterintelligence services failed to warn of this attack.[18] It is time to revisit how we do intelligence, a function of government that some believe to be "flawed by design."[19] We have capability in the SOLIC arena, but our linguistic and law enforcement capabilities are severely lacking. We invest virtually nothing in dealing with major nonviolent nontraditional threats including immigration and environmental threats. Finally, while we have increased our attention toward the electronic battlefield, we have not really done much to protect our home front infrastructure.

PART II—INTELLIGENCE REFORM

Criticism of our intelligence capabilities is not new. As far back as the late 1940s, commissions to review our national intelligence capabilities existed, as shown on Table 1.

YEAR	REVIEW
1949	**First Hoover Commision** • Adversarial relationships between CIA, State, and the military
1955	**Second Hoover Commision** • Counterintelligence & linguistic training deficiencies • CIA to replace State in procurement of foreign publications
1961	**Taylor Commission** • Failure in communication, coordination, and overall planning • No single authority short of the President capable of coordinating the actions of CIA, State, Defense, and USIA[20]
1971	**Schlesinger Report** • "Rise in . . . size and cost [with the] apparent inability to achieve a commensurate improvement in the scope and overallquality . . ." • "Unproductively duplicative" collection systems and a failure in forward planning to coordinate the allocation of resources
1976	**Church Committee** • DCI should have program authority, and monies for national intelligence should be appropriated to the DCI rather than agencies • Recommended second DDCI for Community Management • State must improve overt collection of economic and political data • Raised issue of separating clandestine/covert ops from analysis
1992	**Boren-McCurdy** • National Security Act of 1992 (not adopted, Defense opposed) • DNI, two DDNIs, consolidate DIA and INR analysts with CIA[21]

Table 1. Historical Intelligence Reform Views.[22]

Only the last review sought to modernize and reissue the original National Security Act. Today expert observers are suggesting that not only do we need a National Security Act of 2002, but that this would be a good vehicle within which to establish the Homeland Defense Agency and its authorities.

The National Security Act of 1992, a very promising effort at reform, was headed off by the administration through a compromise led by Senator John Warner of Virginia. A bipartisan commission was appointed. The

House Permanent Select Committee did its own review. The committee's major findings are listed in Table 2.

Tropical Area	Commission on Intelligence	IC21 Study (HPSCI)
Role of Intelligence	Support diplomacy, military operations, defense planning	Too *ad hoc* today, lacks coherence, can be self- serving
Policy/ Requirements Process	State and Defense dominate guidance, consumers group needed	Declining intelligence base and lost focus on future; system-driven
Global Crime, Law Enforcement	Need more coordination of operations overseas, more sharing of information	Need more information sharing and training, global operational coordination
Organization and Communications	DDCI/CIA and DDCI/CM, increases DCI authority	Authorized three ADCIs for major functions of collection, production, infrastructure
CIA Itself	Needs better management at all levels	Must move Centers to DCI level, improve quality of personnel
Budget Structure and Process	Substantial realignment needed to aggregate functions; DCI does not have staff, tools, or procedures for performing budget management	Stove-pipes dominate resources rather than analysts or end-users; CMS should have withholding authority and evaluation ability
Intelligence Analysis	Must improve focus on consumers, on open sources	CIA's core function; assumes departmental capabilities okay
"Right-Size" and Rebuild	Consolidate senior executive service, liberal force reduction	Rationalize NFIP, JMIP, and TIARA,[23] guide by function
Military Intelligence, Support DoD	DoD needs a single *staff* focal point for managing intel support	D/DIA to be Director of Military Intelligence
Technical Collection	Endorses NIMA, need more coordination of intelligence and DoD	Technical Collection Agency and Technical Development Office
Clandestine Service	Merge DoD HUMINT into CIA HUMINT	Separate entity reporting directly to DCI, CIA feeds it
International Cooperation	Burden sharing in space operations	Not addressed, but notes need to buy more open source imagery
Cost of Intelligence	Cost reductions are possible but need better process to find; states 96 percent of USIP is in DoD	States that DoD controls 86 percent of the resources; DCI lacks authority
Accountability and Oversight	Extend tenure of members of the oversight committees	Ease or eliminate tenure limits

Table 2. Summary of 1993-1996 Reviews.[24]

For a number of years, it has been clear that intelligence was not meeting the needs of public programs; that we did not have adequate indications and warning methods for dealing with revolutionary surprise; that our counterintelligence and operational security cadres were well below par; that we did not have an information technology strategy for integrating information across agencies and from different disciplines; that our requirements system was broken; and that our resources were out of alignment—too much money for technical collection and almost none for clandestine human collection, all-source analysis, processing, or counterintelligence.[25] It is also clear that we were spending too much money on technical collection against Russia and China to the virtual exclusion of all else; that we were paying cursory attention to both clandestine and open source collection; and that we suffered from severe mind-set inertia.[26]

Two major deficiencies characterize all Army, Department of Defense (DoD), and other end-user processes. First, the knowledge is not available at any level of command to *triage* internal requirements for intelligence support between classified, commercial, and government sources. Second, there is no open source information channel into each element, for the simple reason that no one has budgeted properly—or created doctrine or force structure—for resolving requirements through the purchase of commercial open sources and value-added information services.[27] The first major systemic deficiency is so severe it calls into question all that we do in the classified world. In brief, absent a structured collection and exploitation effort against multilingual open sources around the globe, it is impossible for the secret disciplines to be fully effective, lacking tip-off and context.[28] The second major systemic deficiency is equally severe in that we do not have any all-source processing environment at all. The various intelligence and counterintelligence elements are severely fragmented, even within their own organizations,

and all the information that is known—including especially raw field station reports—is simply not coming together in any one system from which patterns and anomalies could be drawn out.

In essence, the U.S. Government has chosen to earmark $30 billion a year to go after secrets, while earmarking next to nothing for global multilingual information that is legally and ethically available. Part of the explanation lies in the fact, as reiterated by the Aspin-Brown Commission, that every agency and department of government is responsible for collecting its own open source information. However, the reality is that both the U.S. Intelligence Community, which the Commission found to be "severely deficient" in its lack of access to multilingual open sources, and the various elements of government had over time "given up" on trying to collect, process, and deal with open sources, with one glaring exception: those sources that came to them for "free" from various parties with an agenda to advance. Over time, the U.S. Government has come to rely on a very narrow range of secrets and a very suspect range of open sources.[29]

Missing from this picture is the all-source processing center necessary to properly task all sources and exploit all sources.[30] As we enter the 21st century, we have generally failed to correct all of the deficiencies that have been identified since the 1940s, many of them—such as excessive spending on technical collection—repeatedly pointed out by successive commissions. Problems have tended to be "fixed" by creating new agencies costing even more money, or by throwing additional funds at old agencies that go on to spend the new money with an old mind-set.

PART III—THE NEW CRAFT OF INTELLIGENCE

Today the political environment within which decisions are made has changed, making public intelligence more useful. The old political paradigm for national security was (some would stay still is) unabashedly unilateralist, reflecting a single culture adamant about having its way.

Decisions were made by a small group of leaders relying heavily on secret sources. The new political paradigm, in contrast, is persistently multicultural and "bottom-up," demanding consensus and coordination across national and organizational boundaries. Open sources and methods acquire extraordinary value in this environment.

The information environment itself has changed, in essence "exploding" beyond anything we could have conceived of even as recently as 1994. Internet nodes—and the content that goes with them—is predicted by Dr. Vint Cerf, one of the two fathers of the Internet, to be going from 400 million today to upwards of 3 billion by 2012.[31] This means, among many other things, that we must shift our emphasis from collection to processing. Navigation becomes a vital skill. Knowing who knows[32] and knowing how to filter masses of openly-available information—much of it free, the best of it is available at modest cost to anyone—become the core competencies of the information age.[33] Three areas of emphasis would appear to be important: first, the automation of first-order filtering, but with a very high degree of control and transparency; second, some form of permanent information tagging as to source, time, and location; and, third, historical reach-back.[34]

The reality is that our national security intelligence "system" has isolated itself from 90 percent of the information stakeholders around the world—and especially so from the foreign stakeholders that originate, filter, and validate multilingual information in science and technology, politics, economics, culture, religion. Every topic important to our survival in the 21st century is being pushed away by our current business practices.[35] In combination, our emphasis on "system-high" information technology and on security clearances, classification of everything we think and write, and our 50-year-long obsession with technical secrets from a small number of denied areas, has caused us to ignore and alienate all of these potential partners.[36]

Both our intelligence community and our military community are optimized to treat foreign states as the threat and the target, using a range of complex weapons "over there" and planning a conventional combined arms offense against fixed-ground objectives. That's not the deal, at least as far as bin Laden is concerned, nor will that suffice for the two stark scenarios—the mass break-out scenario or the black-death-in-place scenario. We now find that the private sector is the primary actor in protecting our infrastructure here at home from *individual* actors. Actually our own neighborhoods comprise the "front line" and our citizens are the "forward observers."

What must we protect? More specifically, what must our *domestic* counterintelligence and security personnel be concerned with? Figure 3, which shows a pyramid of key vulnerabilities, seeks to refocus our efforts toward a balanced approach between the physical and the electronic, as well as public health. All three are important.

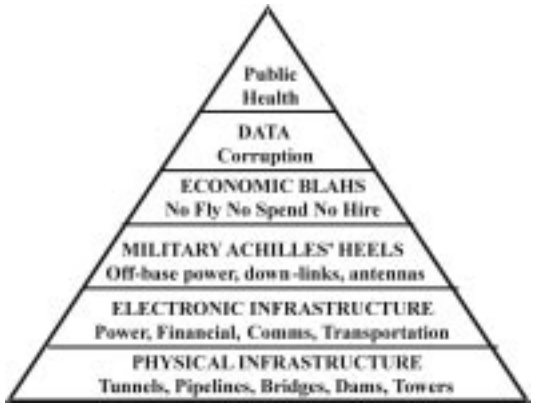

Figure 3. Pyramid of Vulnerabilities.

The harsh reality is that America is not designed to withstand even a small band of suicidal individuals armed with hijacked 18-wheeler trucks, off-the-shelf hazardous materials, and such antitank rockets or other improvisations as they might be able to steal or buy. At the

same time, our public health system has collapsed, and our borders are very porous. We have also failed to think about immigration in a strategic manner. [37] From fuel farms next to I-95 to intelligence community and government agency downlink antennas to the telephone switching stations, dams, bridges, major oil pipelines—even the Panama Canal—these have all been featured in the public discussion since at least 1990. As we seek to orient, observe, decide, and act in defense of our national security and to preserve and further our national prosperity, the speed with which we correct our intelligence deficiencies as well as the speed with which we execute the new craft of intelligence will matter.[38]

The New Craft of Intelligence.

The new craft of intelligence is neither complex nor mysterious. It represents a thoughtful and balanced shift of emphasis from secrecy to openness; from traditional military concerns to concerns about nontraditional factors including water, energy, food, disease, and general sustainability; from current monitoring to historical and cultural contextual analysis; and, finally, from a fragmented community of secret government agencies to a vibrant network that is able to harness distributed intelligence. Above all, the new craft of intelligence is comprehensive, reliable, swift, and *relevant* to the challenges of all threat forms and especially nontraditional threat forms. The new craft of intelligence, properly effected, provides an *asymmetric advantage* in dealing with any challenges, be they violent or nonviolent, state or nonstate, immediate or long term. It will elevate the importance of spies and secrecy, but will do so by focusing this traditional element very narrowly.[39] Most importantly, the new craft of intelligence makes deliberate investments in global history, a shared global open source network, and a home front network.[40] (See Figure 4).

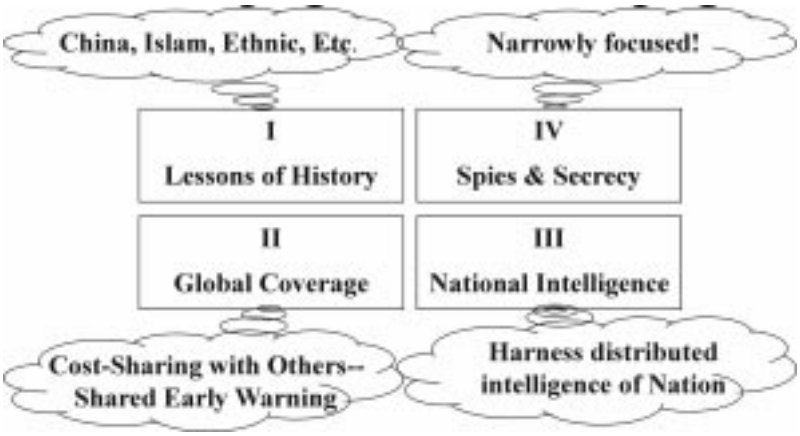

Figure 4. The New Craft of Intelligence.

The first quadrant, the most fundamental, the most neglected, is that of the *lessons of history*. When entire volumes are written on anticipating ethnic conflict and history is not mentioned at all, America has indeed become ignorant.[41] We have failed to honor history, and we will pay the price. Despite the fact that most major government organizations have very talented historians who labor anonymously to keep that organization's past glories well burnished, very rarely does any political appointee or senior policymaker call for the historian to inquire: "What lessons have we learned in the past?" There is an easy fix to this—we must embrace the historian, empower the historian, demand that the historian be a member of the high table that advises the new leadership in each organization—a Presidential Board of Historians would be salutary, as would a national project to digitize, index, and make accessible to the public the major works of Chinese, Islamic, and foreign tribal histories, among others.[42]

The second quadrant is that of *global coverage*. Whether we agree or not with the former and present Directors of Central Intelligence who are on record as saying that our $30 billion a year can only cover the top tier targets (i.e., they do not permit us to focus on the lower tier issues and countries), the fact is that the future wars are being

spawned in the lower tier countries, and the lower tier issues, such as the collapse of global public health and the vanishing of major fresh water supplies, will decide the fate of future generations.

Therefore, let us acknowledge that global coverage by spies and secret means is *unaffordable* and *unachievable* by any single nation. At the same time, let us acknowledge that the bulk of the information that is relevant to lower tier threats is both unclassified and in the private sector—in the hands of corporations and nongovernmental organizations.

The Internet makes possible an alternative model for global intelligence that relies on distributed collection, distributed processing, distributed analysis, and *shared intelligence*. Perhaps more to the point, it permits *burdensharing* and Global Information Management, an extension of the concept of Corporate Information Management—one-time data entry, global access. A structured international project to establish shared current intelligence reports on every country and issue of mutual concern, together with related experts forums, Internet and private database link tables, and multilingual distance learning packages, would go a long way toward *increasing* global consciousness and *reducing* the cost of *basic* intelligence.[43]

The Army could make a major contribution in this arena by working with the theater Joint Intelligence Centers to sponsor a multinational force protection initiative to collect, translate, and exploit open sources of information that are not now available to the British Broadcasting Corporation (BBC) or the Foreign Broadcast Information Service (FBIS). Working with those two activities, the Joint Intelligence Centers, selected defense attaches, and a distributed network of Army reservists and contract civilians, it may be possible to increase by an order of magnitude our indications and warning of instability in the lower tier countries.

The third quadrant requires that we construct a *virtual intelligence community* that brings together the elements of our *distributed* national intelligence. We must harness the full intellectual power of the nation, a distributed network of local and state government officials, corporate officials, military and police officials, nongovernmental officials, journalists, academics, and individual students and citizens—the "intelligence minutemen" of the 21st century." The center of gravity for national security and national prosperity lies now in the private sector and its intellectual property as well as its accumulated knowledge.

As the September 11, 2001, attacks demonstrated so well, we really must take the asymmetric threats much more seriously, for they demand intelligence sharing among federal, state, and local levels of government, and we must devise new means of addressing these needs. Four critical characteristics of the new *national* intelligence community follow:

- It will use the internet as the common communications and information-sharing medium;

- It will default to unclassified intelligence the majority of the time—information can be sensitive or restricted without being classified;[44]

- It will demand the rapid transfer of the proven process of intelligence—requirements definition, collection management, source discovery and validation, multisource fusion, and compelling presentation, to each of these constituent elements of our nation; and,

- It will see every element of government, at the federal, state, and local levels, fully resourced so as to leverage the substantial information sources and services available from the private sector.

The U.S. Army could make an extraordinary contribution to national, state, and local intelligence in this

quadrant. Acting upon its mandate as the lead DoD element responsible for home defense, the U.S. Army and its National Guard elements could establish, in short order:

- A Homeland Security Analysis Center at Fort Belvoir, Virginia, convenient to the various national agencies as well as the Director of the Homeland Defense Agency, former Pennsylvania Governor Tom Ridge. If built around the Land Information Warfare Activity in cooperation with the Intelligence and Security Command, this center could quickly excel at both electronic and physical homeland security threat analysis.

- Community Intelligence Centers (CIC) in each state, manned by a combination of active Army intelligence specialists, reservists, National Guard personnel, and law enforcement specialists. These should be Operational Intelligence (OpIntel) centers capable of maintaining a 24/7 map of the state that is acutely sensitive to crime, including reports of suspicious activities as well as public health and infrastructure information—transportation, power, financial, and communications.[45]

Last, but not least, come *spies, satellites, and secrecy*. The human condition has not changed; there is still great evil in the world, and it is all too easy for evil people to obtain weapons of mass destruction, to carry out electronic attacks on our financial systems, to engage in activities capable of killing hundreds, if not tens of thousands. America and other nations will always need their spies and their secrets, and we honor that need.

On a solid foundation of open source intelligence in the context of history and with the power that comes from tapping into all sources of knowledge within the nation, spies, satellites, and secrets can provide the President with a *decisive advantage*. In the absence of those, however, spies are isolated, satellites are expensive, secrecy is counterproductive, and we lack *intelligence*.

The new craft of intelligence does not seek to diminish or alter the nature, structure, or funding of the classified intelligence community. It does recommend that no less than 5 percent of the classified intelligence budget be spent on open sources and services directly pertinent to the needs of the clandestine human collectors, the covert technical collectors, and the all-source intelligence analysts.[46]

The new craft of intelligence specifically concurs with and adopts the strong views of the Aspin-Brown Commission with respect to the following:

> The Commission believes that intelligence agencies should not satisfy requests for analysis when such analysis could be readily accomplished using publicly available sources, unless for some reason the results of such analysis would require confidentiality or the specific expertise of the analyst would add significantly to the analysis of the open source material.[47]

In other words, the primary responsibility for the new craft of intelligence, for executing the three quadrants that are not secret, and for integrating the secret with the nonsecret, is on the policymaker, the commander, and the acquisition manager—intelligence is an inherent responsibility of command.

Retaining the Proven Process of Intelligence.

The original craft of intelligence, as described by Allen Dulles and developed over time by Sherman Kent and other heroes of the Cold War, provides a proven process of intelligence that is of lasting value and must be transferred from the secret world to the open source world.[48]

Enormous waste occurs when operators and logisticians jump through hoops to satisfy half-baked questions. Perhaps the most vital part of the intelligence process occurs when a skilled intelligence professional interviews the actual decisionmaker to understand the context and concern that must be addressed. It is not an exaggeration to say that this step will double or triple the value of all that

follows. The traditional craft of intelligence is limited in that it focuses only on the classified collection disciplines. The collection management specialty makes a very big contribution with its understanding of what sources might be best able to answer the requirement, in the timeframe desired, at a cost that is appropriate to the need, and with the degree of discretion that is required. The discovery and validation of individual sources precisely tailored to the need is both an art and a science. Being able to find new sources, to recruit them and validate them and then exploit them, is the heart of the traditional craft of intelligence.

Single sources are fragmentary and often misleading. Only a mosaic of multiple sources, built up over time and thoroughly understood by the various analysts involved, will yield a reliable and comprehensive solution to the requirement. Knowing how to substitute sources for one another, or how to use one source to tip-off another for optimal efficiency, is also the heart of the traditional craft of intelligence.

Finally, the traditional craft of intelligence elevates the presentation of the information to a fine art. It must be delivered in a timely digestible manner to the right person, and it must clearly answer the stated requirement in an effective way. Every law enforcement agency, every state and local government office, every federal action officer, every corporate manager, should adopt this proven process. The new craft of intelligence makes this process much more effective by introducing new rules of engagement and a much larger universe of both sources and partners.

The new craft of intelligence overcomes some of the limitations of a unilateralist and monocultural approach to international intelligence, and it is especially strong in overcoming past dependencies on secret or proprietary collection that have combined with deficiencies in processing, translation, and exploitation to produce recurring *surprise*. The new craft of intelligence creates a global community of interest built around national

governments who serve as the portals to their own much-enhanced virtual communities, but offering an architecture that accommodates and empowers corporations as well as nongovernmental organizations, to include academic and media organizations. The new craft of intelligence is the operational manifestation of the American way of "netwar," and can provide a decisive asymmetric advantage from the neighborhood level to the national level, against nontraditional threats.

New Rules of Engagement.

The days of confusing secrets with intelligence are over. The new craft of intelligence carefully distinguishes between *data*, which is the raw text, image, or signal; *information,* which is collated data of generic interest and generally broadcast; and *intelligence*, which is information that has been deliberately discovered, discriminated, distilled, and delivered to meet a specific decisionmaking requirement. Intelligence is defined by the end product, not by the source mix. If the commander needs an unclassified answer in 15 minutes that is one page in length, that is the intelligence objective.

Whereas the traditional craft of intelligence has focused on hard targets, and this is natural for a conglomeration of bureaucracies established during the Cold War, the new craft of intelligence recognizes that *surprise* comes from unanticipated combinations and that the safest strategy for avoiding surprise is to cast a very wide net. The new craft of intelligence demands constant monitoring of all countries and topics, not necessarily in terms of collection, but in terms of "pulsing" and change detection.[49]

The traditional craft of intelligence has focused almost exclusively on secret sources, and within secret sources, very heavily on sources amenable to technical as opposed to human collection. The new craft of intelligence strives to restore the balance between technical and human collection (whether secret or not), between collection and processing,

between production and reflection, and between database stuffing and directed inquires.[50]

Instead of focusing on nationstates or specific organizations, the new craft of intelligence focuses on substate actors and organizations at the branch level. "Two levels down" raises the standard for acceptable intelligence very high—it requires that substate actors be understood at the provincial and county or township level and that organizations be understood in terms of the personalities and resource constraints characteristic of the branch level. This degree of granularity can only be accomplished through the new craft of intelligence and its simultaneous emphasis on the optimization of open source collection (previous rule), on processing (next rule), and on burden sharing (last rule).

Regardless of whether or not secret information is part of the mix, processing matters much more within the new craft of intelligence. There are three reasons for this: first, casting a wide net that is inherently multilingual will increase the amount of material that must be translated and indexed; second, human productivity in the information age depends more and more on computer-aided tools; and, third, only by establishing a digital network for collection, processing, exploitation, and dissemination can the full resources of various governments, corporations, and nongovernmental organizations be brought to bear on topics of common concern such as terrorism and crime.

The "chain of command" characteristic of the traditional craft of intelligence, the old paradigm, has a requirement going from the consumer to the analyst, from the analyst to the collector, from the collector to the source, and then back up the chain. This is the *linear* approach, an approach that is both too slow and too structured for fluid situations where nuances matter. The new approach is the *diamond* approach, such that the acme of skill for an all-source analyst may be the ability to place a consumer with a very complex question in direct touch with a private sector expert

that can create new knowledge—nuanced tailored knowledge—that is "just enough, just in time."

In the age of distributed information, when 80 percent or more of the relevant information is *distributed*, the concept of "central intelligence" loses its meaning. Instead, maintaining the archival files, "knowing who knows," and being able to orchestrate a combination of "just enough, just in time" collection, specialized processing, and just the right mix of analytical talents (online and offline) becomes the core competency. Above all, having the distributed network in place, with trusted relationships and preapproved access, becomes more important than any sort of *central* intelligence organization—we still need a *national* intelligence agency, but it should be the center of a *distributed* network.

The traditional craft of intelligence has tended to fragment content from its context and be largely oblivious to timing. This is true both in the collection cycle and in the production cycle. The new craft of intelligence recognizes that the value of any given information, apart from its relevance to the decision at hand, stems from a combination of the content in context and the content in time. Both collectors and producers of intelligence must be acutely sensitive to the day-to-day needs of their consumers.

The new craft of intelligence respects priorities on the first pass but then shifts to gaps all the way down the line. One pass of Global Coverage (encompassing all lower tier countries and topics) is better than 100 passes on five hard targets and nothing at all on the rest of the world. The new craft of intelligence produces what the consumer needs when they need it, tailored to the context of their need, and by definition created for the individual rather than the organization. The new craft of intelligence does not burn up its analysts with routine production—all production is hand-crafted to support a specific decision, and when not doing tailored production, the analyst should be reflecting, training, traveling, or working in the consumer's spaces to

acquire better contextual understanding of the consumer's needs.

The new craft of intelligence restores the original emphasis on strategic (estimative) intelligence, and adds strategic cost benefits analysis to demonstrate conclusively the value of preventive investments over punitive or reactive investments. The new craft of intelligence recognizes that, in a democracy, the educated public must be addressed and kept informed—the issuance of annual strategic threat assessments and quarterly operational threat assessments *to the public* underlies all other classified endeavors.

The new craft of intelligence elevates the all-source intelligence analyst into service as a manager. Unlike the traditional craft of intelligence where analysts are hired right out of school and "grown" over time, the new craft of intelligence hires analysts at mid-career, after they have achieved a personal standing and complete fluency at the expense of the private sector. To handle secrets, the analyst must be one of America's top ten cited authorities in their given area of expertise. In this context, all analysts become personal branch chiefs, responsible for managing relations with a senior set of consumers; for managing a network of external counterpart authorities; for managing a substantial open source support fund; and for managing the tasking and evaluation of classified assets.

The new craft of intelligence, as a natural outcome of applying the new rules of engagement consistent with state and federal law, will empower all-source analysts with a great deal more control over a great deal more sources and services. Improvements will be seen in four areas: First, every analyst-manager (that is to say, every analyst) will have a substantial sum to invest in external open sources and services. No analysts should be expected to do their own open source collection, processing, filtering, and exploitation.[51]

Second, every analyst-manager will be a "principal" in the Global Intelligence Consortium of participating government and corporate entities with common interests who have contributed funding to the Global Coverage Fund and who share access to the "information commons" or Global Information Bank.[52] Chambers of Commerce, Nongovernmental Organizations, even religious intelligence organizations will be fully willing and participating in the unclassified subject-matter steering groups. Those analysts that manage secret sources for the U.S. Government will also be able to manage burdensharing that gives them access to secret sources managed by other governments, and especially to indigenous clandestine personnel who are better able than our own clandestine officers to achieve results in the lower tier countries.

Third, empowered by these two radical and considerable enhancements to the analysts' "global reach," each analyst-manager will be much more forceful and pointed when tasking classified collection systems. Vacuum cleaning and "target of opportunity" collection will no longer be tolerated or credited. Both technical collection and clandestine collection assets and their managers will be held accountable for delivering performance plans showing expected timing, costs and resulting access, and tailored collection that satisfies the requirement.[53]

Finally, every analyst-manager will be the beneficiary of a very substantial investment in all-source processing and a related analytic toolkit that fully implements the 18 functionalities originally envisioned by the CIA's Office of Scientific & Weapons Research, the Computer-Aided Tools for the Analysis of Science and Technology (CATALYST).[54]

Creating the Global Intelligence Community.

The new craft of intelligence will utilize the obvious benefits of sharing open source information and the obvious leverage that America's great wealth and technical prowess provide to establish a "must join" Global Intelligence

Consortium in order to address topics and targets of common concern. At one level, such a consortium would focus exclusively on unclassified historical and current information—Chinese and Islamic historical doctrine, Third World crisis information, and international weather would be in this group. At another level, at a classified level, the consortium would sponsor at least six international joint stations where indigenous clandestine case officers, allied technical collection personnel, and mixed analyst-managers plan and execute the full gamut of classified capabilities against very specific targets of common concern including terrorism, transnational crime, and toxic dumping. Most importantly, this Global Intelligence Consortium would serve as the coordinator for a distributed network of open source databases and a global network of distributed digitizing and translating activities.

Implementation. A major failing of the entire Chief Information Officer (CIO) movement in the past decade has been its continued obsession with information technology for the sake of information technology. Appointing information technologists as CIOs results in more technology, not in more functionality, a better process or product, or even happier, more productive employees.

In his several works, Paul Strassmann puts this all in perspective. Among the major corporations of America, investments in information technology have generally resulted in a neutral or negative return on investment when calculated in relation to Knowledge Capital, Strassmann's term for the value added by the core competencies of the employees.[55]

As Peter Drucker noted so cogently in late 1998,

> 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 system for top management: the collection and organization of OUTSIDE-focused information.[56]

This technical implementation discussion will focus on key concepts that must attend the new craft of intelligence as we make future investments in information technology. The generally acknowledged need to make major investments in tools for tasking, processing, exploitation and dissemination (TPED) results from an understanding that we are, today, essentially without tools. This is a clean-sheet start on the technical side of the new craft.

First comes process. For starters, the over-all technical process must provide for toolkits appropriate to the analyst's workflow, and not attempt to impose on the analyst draconian training or technical understanding requirements. Second, the over-all technical process must accommodate the human requirements for collaborative work and constant feedback. Third, all aspects of the technical architecture must *illuminate* the many source and service options for the analyst—they should not have to hunt for sources that are "on tap." Fourth and finally, the process must be a "one-stop shopping process" with human help desk, security tracking, and easy-to-use account billing features all built in. The technical process must also recognize that, in a virtual intelligence community, "the system is the product." At a minimum, all raw data input to the system from anywhere must have assigned time and geolocation identifiers.[57] Underlying the entire database must be an instantly accessible military mapping system that gives the analyst immediate access to digital versions of military charts with contour lines and cultural features as well as direct links to all available imagery.[58] This "living database" must allow for product "pulls" at four distinct

levels of analytical interest and in relation to specific military mission areas of interest. A top level country profile should permit rapid access to overview information.

Below we see a deeper look at the kind of information that the "living database" must either contain or be able to access instantly from other distributed databases. The threat does change depending on the level of analysis.[59] Perhaps more importantly, it is possible to arrive at useful insights when carefully considering military, geographic, and civil factors in an integrated fashion.

The technical underpinning for the new craft of intelligence must permit interactive modeling and simulation of force-on-force, using real-world data including weather. It should be optimized to permit the "plug and play" integration of order of battle data from commercial providers, and a major investment should be made in nurturing the emergence of commercial providers of terrorist and criminal order of battle data that they cull from massive reviews of foreign language sources across all relevant countries. If the new craft of intelligence can create two all-source processing "living databases" (or a network of distributed databases that interact in a seamless fashion)—one for open sources of information and one for all classified sources of information—then an order of magnitude increase in the effectiveness of all collection (open and secret) and all analysis (open and secret) should result.

Apart from the human side of implementing the new craft of intelligence, a proper interagency and ideally crossnational approach to shared interactive processing is the single most important initiative requiring command attention. Interactive networks are not simply about data, and especially not just about internal data. Figure 5 shows the "big picture" look at what a global interactive network should be striving to achieve.

Figure 5. Global Information Technology Architecture.

Quadrant I is where most CIOs are stuck. Even there, a combination of proprietary systems and low-rent computers (the lowest common denominator) prevent effective exploitation of what is already entered into the system. Quadrant II is where many are headed, but they still have not realized that until Application Program Interface (API) standards are enforced by law, Microsoft, among others, will make generic achievements impossible. Quadrant III is where the new craft of intelligence strives to make major gains, by creating a global network for sharing the burden of accessing and exploiting all open sources. Finally, Quadrant IV preserves the knowledge that is gained by individual employees, a form of meta-database.

Lastly, we come to the functionality that must be at the finger-tips of every analyst. If we are in the age of information and the knowledge worker is the key to national security and national prosperity, then America needs to impose API standards for transparency and stability and, ideally, sponsor a national generic workstation competition that results in a commercial

solution (or multiple solutions) to this need.[61] Such a workstation is shown is Figure 6.

Figure 6. The All-Source Fusion Workstation.

CONCLUSION

America has entered a new era of warfare and a new era of citizen consciousness. It is now both possible, and imperative, that we sponsor the new craft of intelligence in such a way as to make public intelligence products a vital part of force protection at home. The U.S. Army has an extraordinary opportunity to step out and take the lead in harnessing the distributed intelligence and counter-intelligence capabilities of the full nation, and creating a new doctrinal and technical architecture for integrating open sources of information with classified sources of information.

Management.

Within the Office of the Deputy Chief of Staff for Intelligence, ideally colocated with those responsible for Future Intelligence initiatives, establish a six-person cell responsible for three program activities: 1) Homeland Defense Intelligence Program Management; 2) Government Open Source Program Executive Secretariat;[62] and 3) Future Intelligence Collaborative Environment (Reinforced) Support Activities.[63]

Homeland Defense Analysis Center.

The Army is perfectly positioned to offer Ridge the overnight establishment of a Homeland Defense Analysis Center under the oversight of the Army's Intelligence and Security Command (INSCOM), and fully integrating the Land Information Warfare Activity (LIWA). This center, with no less than 250 new positions structured for 24-hour operations as a matter of sustainable routine, will serve as the central node for all the initiatives that follow.

Homeland Defense Brigades.

Working with existing National Guard units as well as existing Reserve units, the Army could devise a new Homeland Defense Brigade in each state or commonwealth that includes battalions of each of the following functions: electronic defense and response; medical defense and response, including bio-chemical early warning and response; law enforcement auxiliary; natural disaster engineering, including firefighting; staff judge advocate, civil affairs, and public affairs; and intelligence. These brigades would be under the oversight of the operational chain of command, but they must be mentioned to provide context for the following new initiative.

Community Intelligence Centers.

The Army should create for each state under the auspices of the National Guard and conforming strictly to state sovereignty and civil rights concerns, a Community Intelligence Center (CIC) where classified intelligence from national sources, law enforcement intelligence, corporate security intelligence, and citizen information can be fully integrated and managed on a 24-hour-a-day "operational intelligence" basis. This will be a challenging endeavor. Over time, and working closely with existing Center for Disease Control (CDC) and other state and local elements, these centers would serve as a single integrated intelligence and (if desired) command and control facility where state authorities could be assured of full access to local, state, and federal information, including foreign liaison leads.[64]

Digital History and Captured Documents Project.

Responsive to requirements from operational commanders in the field, this project would collect, translate, and digitize essential terrorist, Islamic, Chinese, and other critical knowledge bases. Working closely with the National Drug Intelligence Center (NDIC) and other innovators of law enforcement case filing, the project could rapidly process all the untranslated documents from the original World Trade Center bombing and provide continuing support to all on-going Federal Bureau of Investigation and local law enforcement investigations. Using a web-based network of translators and digitization provided by the state-based CIC, the Army could provide a very nimble and responsive solution to the major obstacle facing homeland defense investigations today.

Regional Open Source Activities.

In close coordination with each of the regional theater Commanders-in-Chief and in cooperation with allies now ready to provide indigenous overt human collectors and

translators, the Army could take the lead in establishing regional open source activities (ROSA) in Australia, with a special focus on Indonesia, Malaysia, and China; in Argentina, with a special focus on Colombia and Brazil; in South Africa, with a special focus on instability throughout that region—and including medical intelligence—and in Turkey, with a special focus on the "stans" as well as the Middle East and the linchpin nations of Iran and Iraq.

Global Information Sharing Consortium.

Drawing heavily on its skilled civil affairs population, and especially the 353rd Civil Affairs Brigade in New York (sponsor of some of the most productive information discussions with international nongovernment organizations), the Army could sponsor a web-based information-sharing network and data warehouse that provide free access to a larger store of global open source information to those organizations, including the U.N., that offer some form of access to their own local knowledge.

Generic Analytic Workstation. A modest investment that brings together the existing accomplishments and future concepts of PATHFINDER from the National Ground Intelligence Center, the Future Intelligence Collaboration Environment (FICE) from Joint Forces Command, and the CATALYST concepts from the now-defunct Central Intelligence Agency project, could, in close collaboration with the National Institute of Standards and Technology (NIST), create a "skunk works" with an antitrust exemption from the Department of Commerce (similar to that given to the Microelectronics and Computer Technology Corporation (MCC) run by Admiral Bobby Inman). We cannot harness the distributed intelligence of the nation, much less the whole earth, until we get to such a generic analytic workstation.

Open Source Intelligence Training Program. The best available handbook on open source intelligence has been produced by NATO and its new field-grade NATO OSINT

Working Group. The Army could take this, along with other useful instructional materials, and create a standard Open Source Intelligence Training Program that specifically addresses sources and methods relevant to law enforcement as well as nongovernmental organizations, including chambers of commerce. This training program could be made available as free distance learning through the web site of the Global Information Sharing Consortium, where it could serve as a magnet for attracting new organizational partners and screening new individual foreign area experts and translators. A special Mobile Training Team, the best the Army has ever assembled, could visit each theater as well as most embassies, and in the process recruit a global network of official U.S. points of contact that might never be assembled if we relied upon traditional messages and bureaucratic initiatives.

All of the above can be accomplished for $125 million a year, which is the amount that senior leaders in the Executive Branch have already agreed is reasonable for a first-year government-wide open source intelligence program—and this was before the September 11, 2001, attacks, and it now adds everything needed for a homeland defense intelligence network under Army leadership. Other initiatives have been dropped to accommodate the more urgent needs for homeland defense intelligence, but these could readily be proposed and funded in future years. They include a Digital Marshall Plan to accelerate the availability of print media from lower tier nations (thus lowering the cost as well as the time needed for Army exploitation of relevant foreign language sources), some form of University of the Republic (to create homeland defense "cohorts" across private sector and government lines), and a global fellowship program (to dramatically increase our access to local knowledge through "adjunct" foreign area specialists who are not U.S. citizens).

The new craft of intelligence takes the traditional craft of intelligence to a whole new level—it offers an order of magnitude increase in what we can collect, process,

understand, and act upon. In doing so, it increases our national security and may well contribute substantially to our national prosperity. There are no better words with which to end this monograph than those of the brilliant and earnest Honorable Harlan Cleveland, former Ambassador to NATO, Assistant Secretary of State, and very learned educator.

> If there was ever a moment in history when a comprehensive strategic view was needed, not just by a few leaders in high (which is to day visible) office but by a large number of executives and other generalists in and out of government, this is certainly it. Meeting that need is what should be higher about higher education.[65]

The new craft of intelligence will provide the sources and methods to meet this need, across the nation and around the world. The Army has the opportunity to lead America into the future by creating the first truly national intelligence community that is structured for "netwar" and ready to fight smart.

ENDNOTES

1. The predominant characteristic of nontraditional and asymmetric threats is their very character—*not* traditional, *not* symmetric. For this reason, as scholars like Dr. Steven Metz and Dr. Max Manwaring have pointed out, *conceptual flexibility* is the core competency of future leaders and the intelligence professionals who support them. The new craft of intelligence is thus the *fundamental* differentiator and factor in achieving asymmetric advantage against nontraditional threats. Max Manwaring, *Internal Wars: Rethinking Problem and Response*, Studies in Asymmetry, Carlisle Barracks: Strategic Studies Institute, September 2001, p. 76; Steven Metz, *The Future of Insurgency*, Carlisle Barracks: Strategic Studies Institute, December 1993.

2. Counterintelligence (or intelligence against enemy intelligence) is a major aspect of the craft of intelligence. When used together with intelligence, the term emphasizes the distinct responsibilities of the two sides of the intelligence coin. When the word intelligence is used alone, it always includes and provides for counterintelligence as a substantive subset of intelligence.

3. Only decisive action by the Federal Aviation Administration (FAA), the order grounding all 3,800+ airplanes in the air instantly, prevented other similar attacks from being carried out against Atlanta, Chicago, and San Francisco. Over half the airplanes were on the ground within 30 minutes at the nearest available airport. This single decision and the heroism of the pilots and the air traffic controllers that got everyone safely on the ground within such a very short time may well have saved 10,000 or more lives and further symbolic catastrophes across America. If the Mossad report to the CIA was correct, that there were 200 martyrs-in-waiting within the United States in August and 19 of them took four airplanes, then a considerable number of other planes may well have been destined for similar fates.

4. The appointment of Army Secretary Thomas E. White to be the first homeland defense coordinator for the DoD, and the restoration of homeland defense as the first of four core military missions, suggests that the Army could play a pivotal role in all aspects of homeland defense, including the adoption of the new craft of intelligence in any Homeland Defense Analysis Center and any nation-wide intelligence network that links state and local intelligence (perhaps via the Guard or Reserve) to national and military intelligence networks. Cf. "Homeland Security in a Pentagon Post," *The New York Times*, October 3, 2001.

5. This monograph will not address the emerging literature on the growing sense that there is a real problem with free market capitalism, except in passing and in relation to the dispossessed billions. George Soros, *Open Society: Reforming Global Capitalism*, Public Affairs, 2000; and Oliver Bennett, *Cultural Pessimism: Narratives of Decline in the Postmodern World*, Edinburgh University Press, 2001, do an excellent job of articulating the main themes of environmental decline, the pathology of capitalism, the end of politics (hostage to corporations and ignored by voters), social disintegration, and the loss of faith in science and technology as savior. Several recent articles critique and expand upon these important themes, among them Madeline Bunting, "Comment & Analysis: The End is Nigh: Most of Us are Transfixed by the Idea that the World is Heading Towards Doom and Disaster," *The Guardian*, August 27, 2001; Faisal Islam, "Business: The Globalisation Debate: Soros: May Day Protestors do have a Point: A New Coalition is Needed to Change the Global Economy in Favour of the Poor, the Financier Tells Faisal Islam," *The Observer*, May 6, 2001, p. 3; Arthur M. Schlesinger, Jr., "A Question of Power," *American Prospect*, April 23, 2001, pp. 26-29; David C. Korten, "The World According to George Soros" (Review), *Tikkun*, March 1, 2001, p. 71; Keith Wilde and R. G. Schulte, "Democratic Capitalism Vs. Binary Economics, *The Journal of Socio-Economics*, March 1, 2001.

6. Robert S. McNamara and James G. Blight, *Wilson's Ghost: Reducing the Risk of Conflict, Killing, and Catastrophe in the 21st Century*, Public Affairs, 2001. The pertinent paragraph on p. 82 is based in part on a conference held at Harvard in 1997. It merits emphasis that those who "hate" America appear to focus on corporations and consumerism, not on the American people and democracy. We need to be sensitive to this distinction. Cf. Benjamin Barber, *Jihad vs. Mcworld: How Globalism and Tribalism are Reshaping the World*, Ballantine, 1996, p. 207.

7. Among the most helpful books in understanding the true perception of America in the eyes of these billions of dispossessed is that of Chalmers Johnson, *Blowback: The Costs and Consequences of American Empire*, New York: Metropolitan Books, 2001. Another key book specific to the conflict between radical Islamists and America *qua* corporate monolith and consumer society is that of Barber on *Jihad vs. McWorld*.

8. The unique legal-dual status of the National Guard opens the possibility of its intelligence officers being simultaneously deputized as law enforcement officers. This would allow them to legally cross-walk national intelligence watchlists against credit card and travel industry databases, and execute such other investigative actions as are legally allowed law officers but not regular military officers.

9. Apart from the obvious dictum that we must manage all the instruments of national power within a grand strategy, there is as yet no structure or practice for doing so. Douglas T. Stuart, ed., *Organizing for National Security*, Carlisle Barracks: Strategic Studies Institute, November 2000, provides an excellent collection of articles from the Army War College's 10th Annual Strategy Conference. Chapter 12, "Presidential Leadership and National Security Policymaking," by this author, focuses on the need for a strategic element within the president's personal staff, as well as for a secretary-general able to marshal the resources of the Departments of State and Defense as well as Justice, for homeland defense and oversea operations.

10. General statements made during his tenure at the Marine Corps University in the mid-1990s when the author served there as a reserve officer.

11. Figures based on a map of current world conflict prepared by Professor Albert J. Jongman, Interim Coordinator of the PIOOM Project, Department of Political Science, Leiden University, Wassernaarseweg 52, 2333 AK Leiden, Netherlands.

12. The Middle East is, of course, important, as is the Latin America region in our own backyard, but these are already clearly identified as areas of interest, and this map focuses on the newer and less-familiar strategic priorities.

13. Water scarcity is depicted in *The State of the World Atlas*, New York: Simon & Schuster, 1981, on charts 53-54. Mineral power is depicted on charts 13-14. Timber power is depicted in the Penguin 1999 edition, on pp. 100-101. Interestingly, population replenishment (or lack thereof) is the focus in the early edition chart 3, while population control is the focus of the later edition on pp. 14-15. The genocide lines are from Dr. Gregory Stanton, whose list of on-going genocide campaigns is at *supra* note 33. Note that China is very much a wild-card—it lacks resources, has over 300 Chinese *cities* that are water-stressed, has a very large population living near the poverty level, and is pressuring Russia from the south with both planned and unplanned migrations.

14. These four paragraphs and Figure 1 are replicated from the author's "Presidential Leadership and National Security Policymaking," Chapter 12 in Douglas T. Stuart, ed., pp. 249-251.

15. It merits comment that the author emphasized transnational crime at the time these words were first written, in early 2000, because terrorism appeared to have been largely suppressed and, in comparison to the costs of transnational crime, was at the time perceived to be "below the line" at the strategic level of net assessments.

16. More recently we have begun to realize the error of our ways. The Associate Director of Central Intelligence for Analysis and Production, Dr. John Gannon, has spoken publicly several times about the challenges facing us in the 2015 timeframe, and he clearly appreciates the national security implications of population growth, migration and immigration, the environment including energy and water supplies, and disease. In May 2000 the administration declared that AIDS is now a national security threat. This is all for the good, but just as it took us 50 years to evolve a national security structure—including the all-important intelligence support structure—so also will it take us at least a decade, if not more, to redirect our sources and methods so as to adequately address this threat.

17. To the extent that the U.S. military was willing to think new thoughts, this threat of information warfare and information terrorism gripped everyone's imagination. Considerable funds have been spent on both critical infrastructure protection and on various service capabilities to achieve "information dominance." Information

technology, rather than intelligence analysis, has been the major defining aspect of the newest fad within the U.S. military (that of Information Operations, or IO).

18. This monograph will not address intelligence failures or deficiencies in detail. The Aspin-Brown Commission (whose recommendations have not been implemented) and over 12 intelligence reform books published in 1999-2001 have amply documented the many issues facing this community. It does merit comment, however, that there were a wide variety of advance leads received by the CIA, the Federal Bureau of Investigation, and the U.S. Secret Service, and none of the leads was either entered into an interagency automated system, or recognized as an indicator of a clear and present danger. We were not able to "make sense" of what we knew.

19. Amy Zegart, *Flawed by Design: The Evolution of the CIA, JCS, and NSC*, Stanford, CA: Stanford University Press, 2000; together with David F. Rudgers, *Creating the Secret State: The Origins of the Central Intelligence Agency, 1943-1947*, Lawrence: University Press of Kansas, 2000; fully describe the circumstances surrounding the birth of the CIA, such that it has never been fully effective. Other elements of the U.S. Intelligence Community, generally created to meet a military need inside the Pentagon budget and culturally oriented toward the Pentagon, are commensurately weak and unresponsive in relation to nonmilitary intelligence requirements.

20. The United States Information Agency (USIA) is the cultural outreach element of the U.S. Government that has been recently absorbed by the Department of State.

21. DNI is Director of National Intelligence, DDNI is Deputy Director of National Intelligence, and INR is the Bureau for Intelligence and Research of the U.S. Department of State.

22. This table was created on the basis of an extraordinarily useful report by Richard A. Best, Jr., and Herbert Andrew Boerstling, "Proposals for Intelligence Reorganization, 1949-1996," February 28, 1996, Congressional Research Service, and included as the final appendix to the *IC21: Intelligence Community in the 21st Century* report of the House Permanent Select Committee on Intelligence, March 4, 1996. This table, and the next, were created for chapter 12 of *On Intelligence: Spies and Secrecy in an Open World*.

23. National Foreign Intelligence Program (NFIP), Joint Military Intelligence Program (JMIP), and Tactical Intelligence and Related Activities (TIARA).

24. Commission on the Roles and Capabilities of the United States Intelligence Community, *Preparing for the 21st Century: An Appraisal of U.S. Intelligence*, March 1, 1996. Also *IC21: Intelligence Community in the 21st Century*, a Staff Study of the Permanent Select Committee on Intelligence, House of Representatives, 104th Congress, March 4, 1996.

25. This section was first published in the *American Intelligence Journal* (hereafter *AIJ*) in the Summer/Fall 1990 issue.

26. *AIJ*, Autumn 1991.

27. The fact that every command spends minor amounts of money on their library and access to the occasional commercial online source of articles is irrelevant. Properly done, each CINC and each Service intelligence center should be spending upwards of $2 million a year *each* on tailored open source intelligence. Once commercial imagery and Russian military maps as well as translation services are factored in, translating a single book from Farsi can cost as much as $30,000. This sum can be seen to be a minimal mandatory amount.

28. For over 5,000 pages from over 500 authorities on open source intelligence in relation to the all-source intelligence challenge, see *www.oss.net*, "Open Archives," containing the *Proceedings* from most of the annual international conferences held since 1992, White Papers by the author, and approximately 4 years worth of the monthly *OSS Notices* on open source developments around the world.

29. The author's second graduate thesis on strategic and tactical information management for national security (Norman: University of Oklahoma, 1987) found that the average embassy collects less than 10 percent of what is legally available for two reasons: only the spies have money with which to reimburse local experts (who are required to commit treason as part of the deal); and in the absence of money, what the average embassy officer can collect in a 24-hour day is severely limited. Worse, the author found that hard-copy routing procedures relegated 80 percent of the 10 percent to the shoe box filing systems of the receiving agencies in Washington, meaning that—and this is not too far-fetched—Washington is operating on 2 percent of the legally available information.

30. The recent report of the commission chartered with reviewing the National Imagery and Mapping Agency (NIMA) found that the lack of investment in Tasking, Processing, Exploitation and Dissemination (TPED) technologies severely limited what could be done with the information collected from our satellites, where we are generally over-invested.

31. Dr. Vinton G. Cerf and Robert Kahn are the two generally acknowledged founders of the Internet. See especially Dr. Cerf's international slide shows on his official web site at *http://www.worldcom.com/generation_d/cerfs_up/index.phtml?grph=1*.

32. Dr. Stevan Dedijer, the father of business intelligence, made this point when he led a delegation of 15 Swedes to the first open source intelligence conference sponsored by the author in December 1992. The fact that 15 Swedes showed up for an open but not advertised event intended largely for the U.S. Government says a great deal about their global early warning network, and their interagency informal communications network.

33. Numerous books have been written on how the information explosion is changing everything, and perhaps 20 percent of them actually have something interesting to say. Three that I have found useful (and reviewed at *www.amazon.com*) include, in order of preference: Regis McKenna, *Real Time: Preparing for the Age of the Never Satisfied Customer*, Cambridge: Harvard, 1997; Philip Evans and Thomas S. Wurster, *Blown To Bits: How the New Economics of Information Transforms Strategy*, Cambridge: Harvard, 2000; and Don Tapscott, *Digital Economy: Promise and Peril in the Age of Networked Intelligence*, New York: McGraw-Hill, 1996.

34. The greatest evil of the digital era is found in its burial of all nondigital information including current and historical experience. Television only recognizes the last 40 years. Media analysts for the *Foreign Broadcast Information Service (FBIS)* sit at their cubicles in Reston, Virginia, and read foreign articles completely out of context—they have no feel for what is actually going on around them. A really superior book that helped me understand these points is that of Bill McKibben, *The Age of Missing Information*, New York: Plume, 1992.

35. I will not focus on network theory or the sociology of creating networks. I do, however, want to acknowledge a useful body of work from John Arquilla and David Ronfeld, who have substantially advanced the dialog in this area. One of their more recent articles is "Networks, Netwars, and the Fight for the Future," *First Monday*, Vol. 6, No. 1, October 1, 2001. The entire issue is at *http://firstmonday.org/issues/issue6_10/index.html*. The new craft of intelligence creates and nurtures networks in order to be smarter, sooner, and broader, than its opponents (themselves adopting networks).

36. "System high" technology is able to handle all compartmented information.

37. The most subtle and subversive form of warfare between cultures is that which is nonviolent, pervasive, and ultimately fragments or takes over the nation being invaded—through immigration. The Break-Out scenario is the extreme manifestation of Irredentist-Immigrant or Group I Warfare. In the absence of immigration controls and commensurate measures to fully integrate new citizens, such as English language fluency being required before acceptance, a loss of national identity and eventual dissolution or reconstitution (e.g., Estados Unidos de Mexico) may result. Drawn from unsigned 3-page paper received in the mail and postmarked Key West, Florida, September 27, 2001.

38. Colonel John Boyd (USAF, Ret.)— the "OODA Loop."

39. In no way should the new craft of intelligence be interpreted as suggesting a draconian cut in funding for secret satellites and spies. While there must be a better balance between what we spend on technical collection and technical processing, from 95-5 percent to 60-40 percent, funding for both spies and all-source analysts must be at least doubled if not tripled.

40. A Homefront Defense Analysis Center (HDAC) is an absolutely vital capability that should be mandated by Congress as part of the legislation that empowers Governor Tom Ridge. In the absence of such legislation with mandated authority over the relevant portions of the bureaucracy, and a dedicated HDAC that can integrate national foreign intelligence, law enforcement intelligence, and corporate security intelligence—as well as gain legal access to credit card and travel industry databases for the purpose of checking all individuals on a new consolidated national watchlist—Ridge will not be effective.

41. Ashley J. Tellis, Thomas S. Szayna, and James A. Winnefeld, *Anticipating Ethnic Conflict*, Santa Monica: RAND, 1997. For a general statement on the terrible decline in American analysis and reflection, see Allan Bloom, *The Closing of the American Mind*, New York: Simon & Schuster, 1987. We have become even more isolated in our interests, and less knowledgeable, in the closing years of the 20th century.

42. A Digital History Program could provide $10 million per year to identify, collect, digitize, and translate essential Chinese and Islamic historical materials, including public pronouncements by leadership, and such other foreign language historical, political, economic, social, cultural, and related information, as needed to create a foundation for rapidly visualizing and modeling both historical patterns and relationships between current information and historical information. Included in this initiative should be an international network of

eminent historians, organized into nodes of three experts for each area of interest (one U.S., one European, one non-European) to serve as a board of advisors and first echelon collection management cell for the acquisition and processing of new historical materials. All of this historical information should be made available via the Internet, in this way creating a genuine "information commons" for multicultural and multinational analysis.

43. As much as $100 million a year could readily be applied by the United States to the following objectives: creation of a Global Intelligence Consortium or official network for coordinating and deconflicting the collection of open source as well as classified information about topics of common concern such as terrorism; the creation of a free global database for storing nongovernmental organization information as a service of common concern; an international training program in open source intelligence collection and exploitation; a wide variety of International Joint Operational Planning Groups (IJOPG) that connect experts on specific countries or topics together as a "virtual task force" available to help any government, or any corporation contributing financially to the ongoing monitoring of the topic in question); four regional open source collection centers, perhaps associated with the major U.S. regional theaters (Pacific, Southern, Central, European); and, finally, a Digital Marshall Plan to subsidize broadband connectivity for lower tier capital cities (including the capitals of provinces) and the accelerated migration of lower tier publishers from analog to digital systems.

44. Through appropriate senior consultations OSS has established that Secret information can be tunneled within the Internet now; that Top Secret tunneling could be approved within the year; and that CODEWORD tunneling is expected to be approved within 3-4 years. The Internet is the new C4I backbone for *all* normal communications within the virtual (national) intelligence community.

45. Some very interesting possibilities exist when you have an intelligence network optimized for unclassified intelligence with respect to Chambers of Commerce and corporations with international contacts. Legal travelers as well as legal referrals that do not have the "tasker" prohibition of classified intelligence suddenly fit into a larger structured collection plan, and the Army gains at least an order of magnitude increase in its "ASK-INT" sources.

46. The generally acknowledged figure for classified community spending on open sources is 1 percent of the budget or $250-300 million a year. Half of that is for *FBIS*. At least $500 million a year should be spent in direct open source support endeavors for the all-source

analysts, and another $500 million a year should be spent in commercial imagery procurement and post-processing to meet theater and service needs for military targeting and mapping applications.

47. Aspin-Brown Commission, p. 17. The general intent of the Commission as reflected throughout the report is for the bulk of "all-source" analysis to move back to the end-user, who is responsible for their own open source collection and exploitation. The U.S. Intelligence Community "all-source" analysts are expected to spend the bulk of their time on classified information, with such open sources as are needed for tip-off or context being provided as needed.

48. Allen Dulles, *The Craft of Intelligence*, New York: Signet, 1965.

49. A commercial example may be helpful here. In the early 1990s, the French steel industry funded a very strong competitive intelligence campaign against other steel industries. In focusing only on steel, they completely overlooked the plastics industry which was busy creating a vast array of substitutes for automobile parts and other traditional steel elements.

50. If applied to the classified community, the new craft of intelligence, as a very rough rule of thumb, would limit collection costs to 50 percent of the total intelligence budget, with one-fifth of those costs, or 10 percent of the total, for clandestine collection, with the other half evenly divided between TPED and analysis. The increased investment in processing, including the use of the Internet for global collaborative work, would help reduce standing armies of intelligence specialists while enhancing the professional qualifications of the remaining analysts and considerably expanding the range of experts from other governments and the private sector that be tasked on an "as needed" basis.

51. Depending on the target and the priority, a variety of external contractors should be available to do foreign broadcast monitoring, down two levels, foreign language polling, document translation and digitization, scenario modeling, and so on. On balance, every analyst should have sufficient funds to maintain at least one full-time open source intelligence specialist and at least two adjunct fellows on modest retainers who are themselves world-class experts in the domain at hand. Naturally there needs to be a central clearinghouse for "best practice, best pricing" information on open sources, and a central contracting office should provide support in realizing economies of scale and ensuring that there is no duplication of effort. The analyst, while subject to oversight, will have the last word on how the open source money is spent, providing the programs adhere to the coordination

process to optimize complementarities within the National Intelligence Agency as well as between participating organizations in the global intelligence consortium.

52. Such names are notional. The bottom line is that there needs to be an Internet-based means of coordinating common interests, and some form of clearinghouse, both for the application of funds and for the processing of open source information that is meant to be shared.

53. Under this approach, case officers and collection managers who develop the performance plans will receive equal credit (or disgrace) with those who execute it over time—instead of pressing for gang-plank recruitments to run up the numbers—for those few officers that still are allowed to recruit, there will be phased operations with very high security, and a team approach to clandestine and covert technical operations.

54. These are discussed in detail in the final technical notes. Dr. Gordon Oehler, then Director, and Ms. Diane Webb, a brilliant young analyst, were instrumental in devising both an extraordinary requirements document and a strategic implementation plan. Their vision was destroyed when CIA's "information technology" managers decided that the "dumb terminal" was to be the standard CIA workstation and forbade any further investments in object-oriented programming and Sun workstations. That one decision destroyed whatever hopes the U.S. Intelligence Community might have had for an advanced collaborative environment in the 1990s. The closest thing we have today is PATHFINDER at the National Ground Intelligence Center, a kludge that was great in its time but needs to be completely redone, and the Future Intelligence Collaboration Environment Foreign Broadcast Information Service at Joint Forces Command, which lacks the rigor and diversity of the original CATALYST requirements statement. Combining the two (PATHFINDER and Future Collaborative Intelligence Environment [FICE]) under a new Army initiative to implement CATALYST as part of its creation of a Homeland Defense Analysis Center could conceivably restore this urgently needed set of capabilities to all analysts in the U.S. Intelligence Community. At the same time, at the very highest level, the ICMAP project to establish a multi-INT tasking and collection management system, while initially limited to signals and imagery intelligence because those are the only disciplines with structured requirements databases, should eventually be expanded to include open source intelligence as well as all forms of clandestine or secret intelligence available from human sources including liaison. The U.S. Army could make a real contribution if it chose to take on the fertile and unattended area of legal travelers and community or mass refugee debriefings.

55. Cf. Paul Strassmann, *Information Productivity: Assessing the Information Management Costs of US Industrial Corporations*, New Canaan, CT: Information Economics Press, 1999. His other major works are equally applicable to the new craft of intelligence from the technical perspective. Cf. Paul Strassmann, *Information PayOff: The Transformation of Work in the Electronic Age*, Detroit: Free Press, 1985; and *The Politics of Information Management: Policy Guidelines*, New Canaan, CT: Information Economics Press, 1995. Strassmann was the CIO of Xerox Corporation and later the Director of Defense Information for DoD.

56. "The Next Information Revolution," *Forbes ASAP*, August 24, 1998, p. 46.

57. Most data will have multiple identifiers, e.g., start point, interim points, and end points for a ship traveling from Thailand to Iran.

58. The current proposed solution of Geographic Position System (GPS) coordinates and image maps is *unacceptable*. The difference between an image map and a military chart is the man-years that have gone into data extraction and the creation of a value-added product that clearly shows to anyone the precise terrain configurations, cultural features, etc.

59. This is discussed in detail in *On Intelligence*, p. 149.

60. The Army could make a difference. If the Joint Forces Command project to create a FICE were fully integrated into an Army project office that migrated PATHFINDER functionality while devising generic solutions for each of the CATALYST functions, this new workstation, developed in partnership with the commercial providers of the elements, could then be utilized in the various state and local Community Intelligence Centers as well as the Homeland Security Analysis Center, and perhaps even at the new NATO Global Cover. Some have proposed a Center for Installation at Joint Analysis Center Molesworth.

61. The following language has been submitted to Congressional authorities with respect to open source intelligence:

> The Congress is deeply troubled by the continued reduction in resources accorded Open Source collection, processing and analysis by the Intelligence Community in general, and by the Central Intelligence Agency in particular and the consequent deterioration in the availability of open source materials to policymakers

> and analysts alike. The Foreign Broadcast Information Service is the most visible, but not the only, example of neglect by the Intelligence Community of the demonstrably most cost-effective sources of intelligence. The Congress is convinced that a single, separate, comprehensive, healthy Community-wide Open Source Program, subject to separate review as an independent program in the National Foreign Intelligence Program, NFIP, with a strong, independent program manager of stature, acceptable to both the Legislative Branch as well as to the Executive is required, and the Director of Central Intelligence is requested to move expeditiously to bring about these needed changes in this continuing area of Congressional interest. The Congress further notes that the bi-partisan commission established to review the roles and missions of the intelligence community specifically charged the consumers of intelligence—the agencies and departments of the government not within the intelligence community—with responsibility for meeting their own intelligence needs when those needs could be addressed by publicly available sources. The Congress therefore encourages the Executive to consider the establishment of a Government-wide Open Source Coordinating Committee, perhaps chaired by the Department of State, and working closely with NFIP Open Source Program Manager to achieve Global Cover while avoiding duplication of effort.

No matter what open source initiatives are eventually sponsored by the National Foreign Intelligence Program, the Army is responsible for its own open source solutions and must make provision for an independent program. In the absence of any expression of interest from DoD or the Department of State, the Army has an opportunity to provide leadership for the rest of the Executive, and in this way achieve primacy in the global open source intelligence initiatives that are essential to both force protection and force structure, acquisition intelligence.

62. This six-person cell might consist of a senior executive service special assistant to DSCINT, assisted by two GM-15s, two GS-13s, and a GS-9-11. All of the positions could be included within emerging legislation for homeland security support activities. All other personnel support proposed in these various initiatives is assumed to be achievable from either existing redirected manpower, or special homeland security legislation. The reality is that the new craft of intelligence should permit considerable manpower savings across all

DoD intelligence rosters. The specific future intelligence support initiatives are listed last, after the homeland intelligence initiatives.

63. These centers should have robust training elements as well as special cadres of active Army innovators who can create doctrine and protocol on the fly, working across state lines and in close coordination with INSCOM. Once the Centers are operating, a very strong Army community relations and training program could be activated, one that takes training teams into every single township to work with local law enforcement as well as to hold town hall meetings that fully educate and inspire individual citizens who then become "intelligence minutemen."

64. Harlan Cleveland, *The Knowledge Executive: Leadership in an Information Society*, New York: Dutton, 1985, p. 203.

U.S. ARMY WAR COLLEGE

Major General Robert R. Ivany
Commandant

*****

STRATEGIC STUDIES INSTITUTE

Director
Professor Douglas C. Lovelace, Jr.

Director of Research
Dr. Steven Metz

Author
Mr. Robert D. Steele

Director of Publications
Ms. Marianne P. Cowling

Publications Assistant
Ms. Rita A. Rummel

*****

Composition
Ms. Kimberly A. Rockwell

*****

Cover Artist
Mr. Gary L. Johnson