CHAPTER 12

PRESIDENTIAL LEADERSHIP AND NATIONAL SECURITY POLICYMAKING[1]

Robert D. Steele

Background

The Ninth Annual Strategy Conference, held at the U.S. Army War College in 1998, addressed the theme of "Challenging the United States Symmetrically and Asymmetrically: Can America be Defeated?" In the course of that event, a number of speakers and participants, including the author, reflected on our existing policymaking process and our existing force structure, but without making recommendations for specific changes.

In the largest sense, the Ninth Annual Strategy Conference called into question every aspect of *Joint Vision 2010* and clearly identified a need to come to grips with several asymmetric threats for which our existing force structure is not well suited as a primary defense. A summary of the conference was subsequently published and is readily available online.[2]

In the aftermath of last year's conference, and again at the invitation of the Army War College, the author undertook the task of considering and integrating three aspects of presidential leadership and national security policymaking:

1. Implications of the symmetric threat;
2. Organizational pathologies in policymaking;
3. Potential Information Solutions.

"Presidential Leadership and National Security Policymaking", in Douglas T. Stuart (ed.), *Organizing for National Security* (Strategic Studies Institute, U.S. Army War College, 2000), pp. 245-282.

Out of that reflection and in keeping with guidance to the effect that one should seek to provoke with "big ideas" that might or might not be immediately or practically amenable to adoption, the author selected the following three ideas for presentation to the Tenth Annual Strategy Conference:

1. Four threat types need four forces after next;

2. Must modify White House staff and leadership method for three departments;

3. Need a national information strategy and a virtual intelligence community approach.

When considered together, these three ideas suggest that we must simultaneously reinvent how we think of the threat, how we organize to deal with the threat, and how we communicate both internally and externally as we make plans and execute operations to confront the threat. At root, our challenge is neither technical nor financial but rather intellectual—how do we modify our perceptions, our information collection, our information processing, and our information sharing so as to permit the president to be much more effective in understanding the threat, confronting the threat, and neutralizing the threat?

Setting the Stage.

As we consider how best to restructure the manner in which the president provides leadership with respect to national security matters as well as how that leadership is implemented, we must face three realities.

First, the Department of Defense (DoD), whatever course it is directed to follow in the early decades of the 21st century, is severely underfunded. As one distinguished former Secretary of Defense stated in congressional testimony early in 1999:

> . . . the course on which we are now embarked involves increasing strains and growing costs in the short term, and is unsustainable in the long run.

> . . . we shall need gradually to increase procurement outlays to $100 Billion per year (from $40 Billion).
>
> (this does not address) homeland defense . . . which) would include protection against chemical and biological weapons, protection of the critical infrastructure against cyber attacks, space control . . . and certain other areas.[3]

Of special interest to us all is the noted reference to the fact that "traditional" DoD funding shortfalls are being put forward that do not provide for homeland defense. The concepts and doctrine as well as the legislation needed to determine who is responsible for homeland defense, and how that is handled in relation to DoD as well as other departments of government, do not exist.

Second, even if the president were to choose a rational course and seek to make substantive changes in how we make policy and execute national security initiatives, it will take many years—from 5 to 25—before such change is agreed to by Congress, accepted by the public, and fully institutionalized.[4]

Third and finally, we come to the complex nature of bureaucracy. No matter what the president may decide and what Congress may legislate, ultimately it will take years to effect substantive change within the U.S. Government bureaucracy if we adhere to traditional forms of change—this paper proposes a nontraditional solution that can be implemented immediately.

Four Threat Types.

As the United States prepares to enter the 21st century there is much discussion about *Joint Vision 2010* and the "force after next." Unfortunately, the net assessment process, so well-regarded during the Cold War, has failed us. Furthermore, the Revolution in Military Affairs (RMA) is nothing more than a perpetuation of our fascination with technical solutions, and fails completely with regard to the much more complex issues of human conflict, culture,

history, diminishing resources, and **sustainability**. We ran out of precision munitions in 8 days during the Gulf War. The North Atlantic Treaty Organization (NATO) ran out of precision munitions for Serbian attacks in just three days. There are those who feel that our stocks of conventional ammunition for plain infantry are also severely inadequate.

The net assessments process of the 21st century will have to deal with four threat types, not one; it must be able to deal easily with both domestic or home front issues that are not obviously military in nature; and it must also deal with the **human factors** associated with avoiding as well as deterring threat conditions from arising both at home and abroad. By human factors I mean historical, cultural, social, and psychological intelligence, four forms of intelligence at which we are especially poor.

Figure 1 shows that each threat type relies on different forms of power, different forms of concealment, and different objectives. At the same time, we see that between the four **types** of threat there are also four different **kinds** of nontraditional conflict.

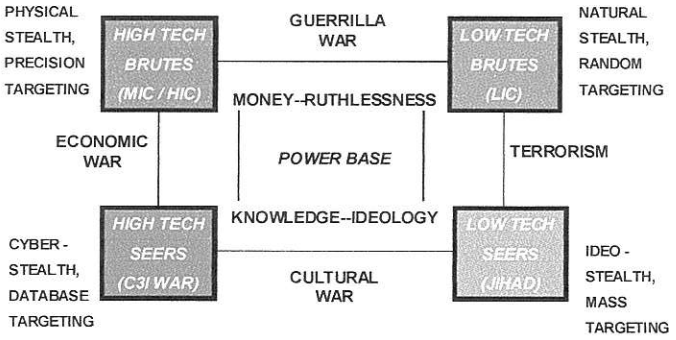

Figure 1. Four Threat Types.

High-Tech Brutes—The Violent State Threat.

DoD and the U.S. intelligence community dedicate the majority—well over 80 percent, if not 90 percent—of their resources to training, equipping, and organizing forces focused on dealing with the "high-tech brute," the violent state.

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.

This is the **only** threat that we focused on during the Cold War, and this 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 enemies, also represent this kind of threat.

This is 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 Non-State Threat.

The "low-tech brute" is violent but generally does not represent a state. Transnational criminal gangs present both defense and intelligence agencies with a threat which is extremely difficult to detect in the absence of a pervasive human intelligence network. This type of threat 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" (LIC) threats for which Congress wisely created the Special Operations

Command and the new Special Operations and Low Intensity Conflict (SOLIC) Program, the low-tech brute is not state-sponsored but rather 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.

Perhaps more to the point, our national security structure—in policymaking terms, in acquisition terms, and in day-to-day operational capability terms—is not geared to effectively challenge this threat class.

Low-Tech Seers—The Non-Violent Non-State Threat.

This "threat" class is not inherently violent although some of its extremist elements may be. It should be viewed primarily as a challenge 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 non-state groups. At root, this threat class is about water, food, and freedom from fear.

Our intelligence community, with the tacit if not the active consent of our national security policymakers, has 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 non-governmental study.

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 Auto-Immune Deficiency Syndrome (AIDS) is

now a national security threat. This is all to 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.

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 hand, 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.

Let us take each in turn. Winn Schwartau was the first to warn America publicly and effectively about the vulnerability of our critical infrastructures, with his books *Terminal Compromise* (1990) and *Information Warfare: Chaos on the Electronic Superhighway* (1994). I myself issued a press release in August 1994 documenting the urgent need for a $1 billion a year investment in critical infrastructure protection. We have a very long way to go before our financial, transportation, power, and communications systems are safe from attack because we have spent decades building computer-driven systems that "assumed" there was no threat other than normal

operational inefficiencies. The entire insurance program for such systems is geared toward "acts of God" and not acts of man. The moment one contemplates vulnerabilities to deliberate human attacks on our most fundamental electronic systems, the risk of catastrophe increases by several orders of magnitude.

We also have a grave problem in dealing with individual insider attacks against all manner of electronic systems because no one ever contemplated the possibility that a trusted employee would deliberately tamper with basic computer software and hardware. Fully 20 percent of our losses in the electronic world are attributable to insider attacks that are motivated by either dishonesty or a desire for revenge. This is four times the losses from outside attacks.[5]

Finally, we come to the whole issue of what comprises appropriate "due diligence" on the part of both the manufacturers of computer hardware and software, and on the part of organizations that install and administer electronic systems on behalf of their stockholders, employees, or members. The reality is that there are no standards today. There is nothing comparable to the accounting and other fiduciary standards for electronic systems. We are still operating our critical infrastructures on the basis of "buyer beware," or "as is" without warranty. This is completely unacceptable since the center of gravity for national security is now in the private sector—in our intellectual property and in our critical infrastructures.

Existing Organizational Pathologies.

As we contemplate presidential leadership options in the national security policymaking process, we quickly identify three major problem areas:

First, the National Security Council staff structure is too limited. It is formed along regional and issue area lines that are undeniably important, but not staffed in consonance

with the emerging fault lines—the environmental element, for example, has the fewest people assigned to it, and the senior position is too easily left vacant.

Second, we have schisms among the three major Departments dealing with national security: Defense, State, and Justice. As now managed and organized, they no longer provide the United States with the most effective arrangements for: defending our population, resources and interests; for exerting necessary influence abroad; and for dealing with individual and gang threats to our prosperity and personal security. The schisms between Defense, State, and Justice are of three kinds: conceptual, financial, and informational.

1. Conceptually we have not yet devised common approaches for dealing with emerging crises such as Burundi, Somalia, Kosovo, Sierra Leone, and Sri Lanka—we are especially poor at early warning, at early resolution or deterrence, and at transitioning from diplomatic to enforcement to military means;

2. Financially we still have the bulk of the money invested in standing armies that are increasingly hollow in both personnel and technical terms; and

3. Informationally we do not have an integrated operational, resource management, or intelligence system adequate to the task of harmonizing cross-departmental inputs, decision processes, and outputs.

Third, and finally, we have a strategic vacuum overall, with no element on the National Security Council having a clear mandate and the necessary resources to marshal for the president and the Cabinet the necessary mix of private sector and other capabilities through which to achieve deep historical and cultural understandings while also assuring access to the widest possible range of multi-lingual content.[6]

Where we see major gaps in the existing White House staff structure are: with respect to policy development at the interface of external requirements and internal

capabilities; with respect to the deliberate introduction of "grand strategy" as well as deliberate net assessments and operational control over integrated defense, diplomatic, and transnational justice initiatives; with respect to much improved national intelligence capabilities that fully exploit open sources of information; and with respect to improved control and coordination of national investments in research.

General Organizational Changes.

Three kinds of organizational change are recommended to improve presidential leadership with respect to national security policymaking.

First, the National Security Council staffing plan needs to be modified to achieve the following objectives:

1. Provide for equal focus on each of the four threat types;

2. Provide for cross-cutting staffing between security and competitiveness issues;

3. Significantly upgrade the role of intelligence in the White House staffing process;

4. Introduce a dedicated strategy element co-equal to the policy and intelligence elements;

5. Introduce a national research element co-equal to the other elements.

Second, and this would naturally require congressional support in the form of legislation, establish the position of Secretary General for National Security. This position would have executive authority over the Secretaries of Defense and State as well as the Attorney General, and would thus be able to better realign resources and integrate programs of common interest. One of the three individuals, ideally the Secretary of State, could, if desired, be "double-hatted" as Secretary-General, if the first incumbent is to be considered a pathfinder in testing this idea.

Third and finally, we must develop an integrated Net Assessments and Operations Staff under the cognizance of the Secretary General for National Security.

These suggested changes avoid major organizational restructuring, avoid any dislocation between the existing executive structure and existing legislative authorization committees, and avoid any major new programmatic initiatives.

At root, these suggested changes are built on three simple principles:

1. Put one person in charge of the three Departments at the policy and resource level;

2. Provide for the needed day-to-day decisiveness regarding cross-departmental activities, personnel assignments, and incremental resource realignments; and

3. Provide for the needed information system integration, especially with regard to shared operational and intelligence information.

Recommended National Security Council Staff Changes.

The existing staff arrangements in the NSC handicap the president in the following ways:

1. national security and competitiveness policy are not always reconciled—some would even say never;

2. national intelligence is severely limited in its ability to exploit open sources of information and harness distributed private sector and international expertise on behalf of the president and **public** policymaking;

3. we have no global strategy office nor any means of providing continuing education to presidential appointees and their private sector counterparts—we have no effective means of "thinking in time" or across cultural and religious and ethnic boundaries;[7]

4. national research is fragmented among departments and special programs.

Block and wire diagrams are an unfortunate but necessary evil. Figure 2 is intended to illustrate some basic alterations in our concepts for approaching presidential leadership with respect to national security policymaking.

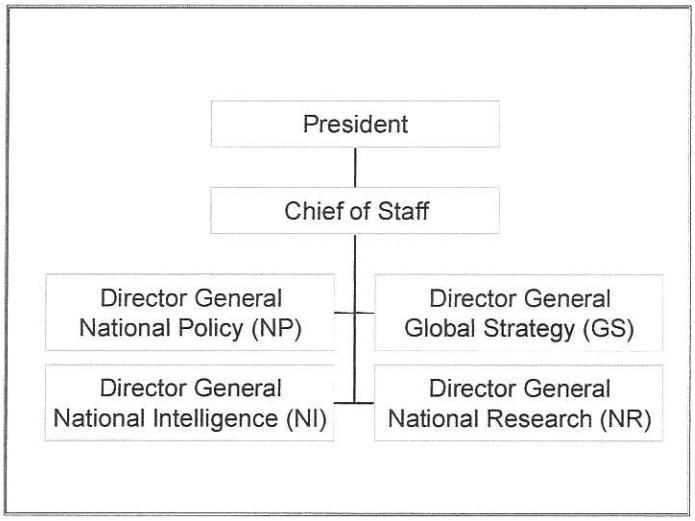

Figure 2. Top-Level Presidential Staff Leadership Positions.

The most basic aspect of a new approach to presidential leadership must be reflected in the integration of national policymaking between national security and national competitiveness together with the simultaneous elevation of global strategy (more properly "grand strategy" but the pundits would take unfair advantage), national intelligence, and national research to the top table. We will discuss each of these blocks in turn.

National Policy.

Figure 3 illustrates an approach to national policymaking that provides balance between three major tracks in national policy: security, competitiveness, and treasury, while also providing for directed attention to each

of the four threat types. Perhaps most importantly, each threat type has its policy counterpart in each of the three tracks.

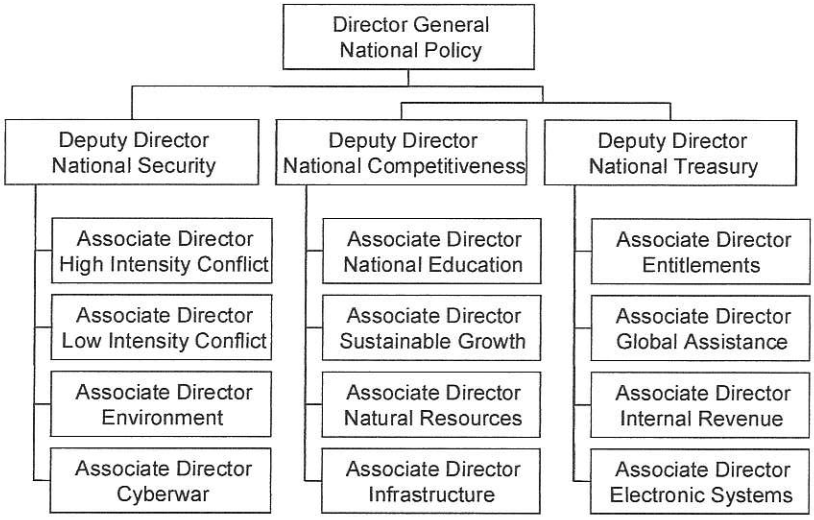

Figure 3. Balanced Approach to National

Ideally, what will emerge out of such a staffing approach is a matrixed policy, planning, and programming process that specifically charts national treasury, national competitiveness, and national security investments in relation to one another.

A situation like Kosovo, for example, would have inspired, several years before-hand, a deliberate calculation of the costs of substantial foreign assistance to include resettlement funding intended to avoid the genocide that has occurred, versus the costs of an after-the-fact aerial bombing campaign seeking to limit the genocide and the consolidation of Serbian power.

Such a staff approach would place a very high value on understanding and utilizing non-military sources of power while also appreciating the degree to which others can use non-military sources of power to affect U.S. national security and U.S. competitiveness.

Global Strategy.

David Abshire has written an entire book on what a strategic element might look like if placed within the National Security Council.[8] His thoughts on the need for an autonomous oversight body for strategic thinking run counter to the popular misconception among policymakers that they can handle strategic thinking *en passant*.

Figure 4 suggests a distinction between broad and independent global strategizing and integrated response management. The global strategy arm is provided with international strategic council as well as a global reserve for providing recurring independent looks at long-range issues. The global strategy arm should have the flexibility to undertake special projects while also being responsible for recurring leadership retreats at which a mix of executive, legislative, and private sector leaders would review a given strategic question.

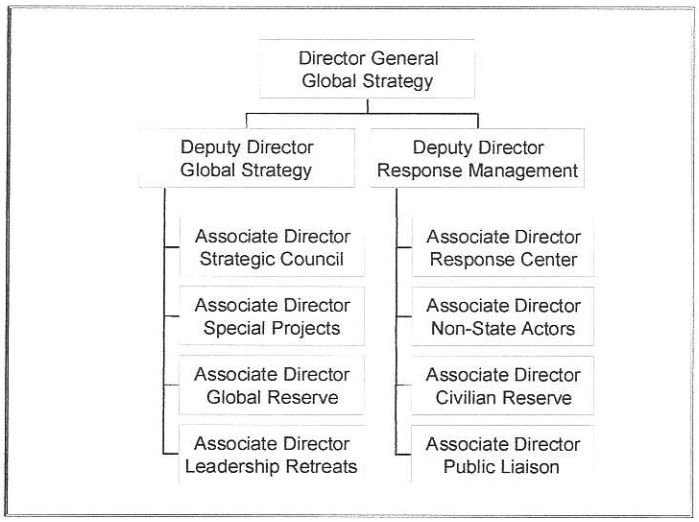

Figure 4. Enhancing Presidential Capabilities for Strategic Action.

On the response side, we move away from the popular term "crisis management" and provide for a more balanced and integrated response capability. The Response Center

intelligence community, Net Assessments, National Security Operations staff and others. The Response Center

equipped, and organized to leverage people—a civilian reserve of experts, the mass media, and large non-state

National Intelligence.

The national intelligence community, traditionally **secrets**, is no

relation to either national security—its focus during the Cold War—or national competitiveness and electronic

There is nothing wrong with the very good people or the very good process embodied in national intelligence. Where

organization, resource trade-offs, and outreach to both the U.S. private sector and to other international intelligence

In the absence of any internal reform responsive to the Aspin-Brown Commission, we must return to legislatively

leading the charge for a complete makeover of our national intelligence community.

The fundamental proposition in the Figure 5 is that our existing classified intelligence community is good and

not good enough to fully satisfy presidential requirements for what joint doctrine calls Relevant Information. The president needs a Director General for National

routine staff capabilities while overseeing the following substantive enhancements.

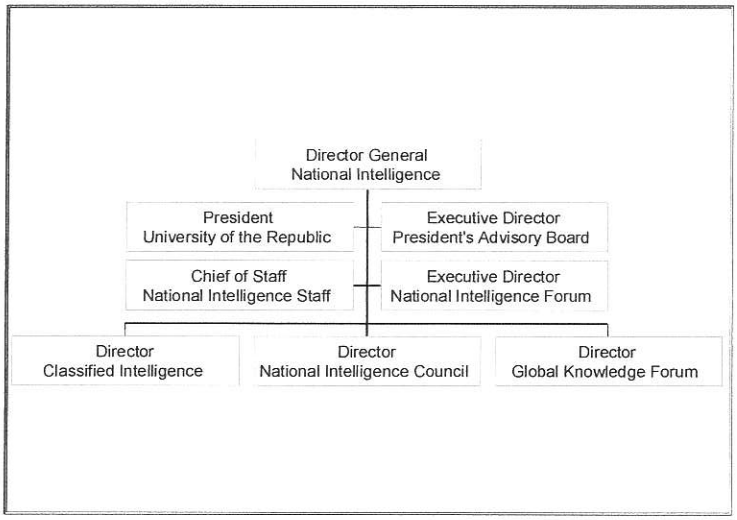

Figure 5. Enhancing National Intelligence Support to the President.

1. Elevation of the National Intelligence Council to a role co-equal to that of the entire classified intelligence community. This larger body of perhaps 60 experts would provide direct support to the president, the Cabinet, and congressional leaders.

2. Creation of a 60-person Global Knowledge Forum with a budget of between $1.2 and $1.5 billion a year with which to acquire open source intelligence on behalf of the president and the executive departments as well as the classified intelligence community.

3. Establishment of a 15-person administrative faculty for a University of the Republic charged with bringing together leadership "cohorts" across government and private sector lines.[11]

National Research.

Both national security and national competitiveness depend heavily on national research. The problems with duplicative waste (government not knowing what private sector has already mastered) have gotten out of hand, especially in the high-profile Critical Technologies arena.

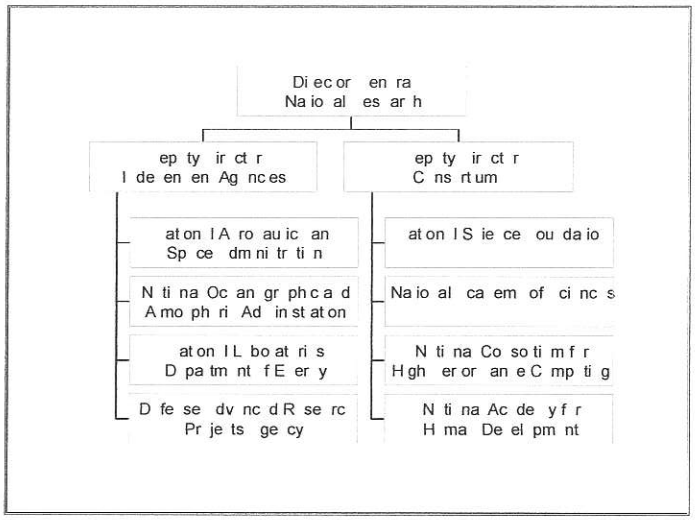

Figure 6. Establishing Presidential Leadership Over Research.

Figure 6 proposes one response to this challenge. This staff element will provide for presidential leadership over research, with one half of the staff serving to better coordinate government investments in directed research, while the other half of the staff will improve the ability of government to work jointly with selected private sector partners in a variety of consortiums exempted from anti-trust actions by the Department of Commerce.

A National Academy for Human Development is suggested because the United States is spending too much money on technology and not nearly enough on human factors.

By placing this staff at the presidential level instead of the departmental level, opportunities for presidential leadership will be enhanced in other ways. The other staff elements (national security, national competitiveness, national treasury) will be better able to matrix their requirements away from the parochialism of the departments.

Cabinet and Operational Changes.

Apart from changes within the president's immediate staff, this chapter recommends only two other changes of significance. First, and this would require congressional legislation, we should acknowledge the complexity of the inter-relationship between the three major departments responsible for national security and put a "human in the loop." Specifically, it is recommended that a Secretary General for National Security be placed above the Secretaries of Defense, State, and the Attorney General. The latter three would remain members of the Cabinet and retain all of their previous prerogatives.

We must mention General Colin Powell here. Regardless of who wins the presidential election in November 2000, it would make sense to appoint Colin Powell as Secretary of State and also as the first Secretary General for National Security, with the South-Central campus, adjacent to State, as the shared national security staff facility. His stature and good will would comfort both the public and the international community as we experiment with this new system. The prestige of State would be elevated, Defense would be under control, and Law Enforcement would receive attention from a leader of great *gravitas*.

Secretary General for National Security.

The Secretary General would serve as a presidential surrogate in addressing the constant day-to-day decisions that require guidance in order to rapidly resolve issues of policy, planning, and programming within the larger context of the budget submitted to Congress by the president and appropriated by Congress for operations. No more than 10 percent of any one department's budget need be subject to administrative reallocation.

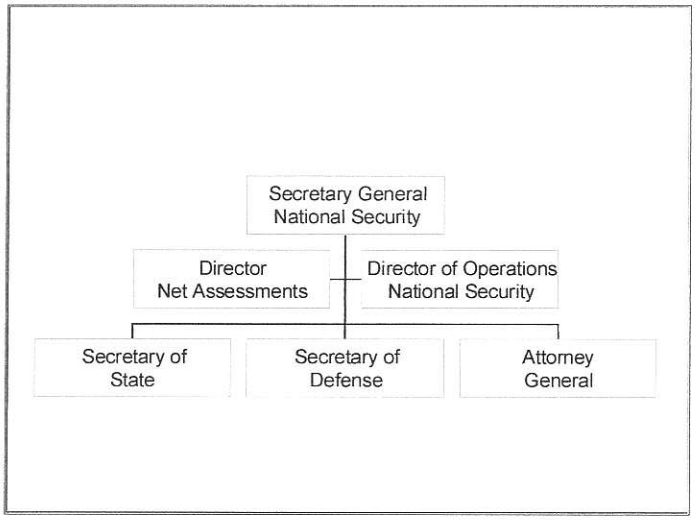

Figure 7. Enhancing Presidential Leadership for National Security.

The Secretary General would focus primarily on the larger policy issues where the secretaries themselves have not been able to come to rapid resolution, and would serve as a means of integrating national security policy making across departmental boundaries.[12]

Integrated Net Assessments and Operational Direction.

Second, the Secretary General would require both an integrated Net Assessments staff, and an integrated Operations staff. Both could be built around a very modest cadre of the "best and the brightest" drawn from each of the three departments to create truly inter-agency capabilities.

The Net Assessments staff, to be elevated above the three departments and given a substantial budget for conducting net assessments in relation to each of the four threat types (to include relative homefront vulnerabilities) would be the primary means by which the Secretary General would examine alternative options for proposing to the president new capabilities and realignments of resources between the three departments.

1. The existing DoD Net Assessments staff would continue to focus on conventional threats and the Revolution in Military Affairs.

2. A new element would focus exclusively on Special Operations and Low Intensity Conflict and would include a mix of paramilitary, peacekeeping, and transnational law enforcement experts.

3. Another new element would bring together experts on major religious and ethnic groups as well as environmental issues, and focus on assessments of alternative timelines and costs for precluding major clashes between large groups of non-state actors.

4. Finally, a new element would be added, which would focus upon a mix of trade and technology competition, economic espionage and information warfare.

Although the Secretary General should have the authority to realign up to 10 percent of any Department's resources in any single fiscal year, multi-year initiatives and major realignments would have to be submitted through the president's budget process and approved by Congress.

At the same time that the Secretary General would require a Net Assessments process, there would also be required a joint Operations staff. A portion of the existing Joint Staff could be assigned as the cadre for this element. Modest in size, its role would be to serve as an operational interface to the three departments, the national intelligence community, the Net Assessments staff, and the presidential staff.

This staff, also, would be organized by threat type, and help bring together inter-departmental resources applicable specifically to each threat type. A significant mission for this operational staff would be to recommend "on the fly" adjustments to departmental programs.

Budget Realignments.

Depending on who is counting what, the DoD budget ranges from $250 billion to $270 billion per year (with new construction) to over $300 billion a year (with DoD-controlled national intelligence elements). Regardless of whether or not the United States gets the additional procurement funds that many concerned leaders have advocated, some form of interim adjustment of DoD priorities must be made, to allow us to develop minimal mandatory capabilities against emerging threats.

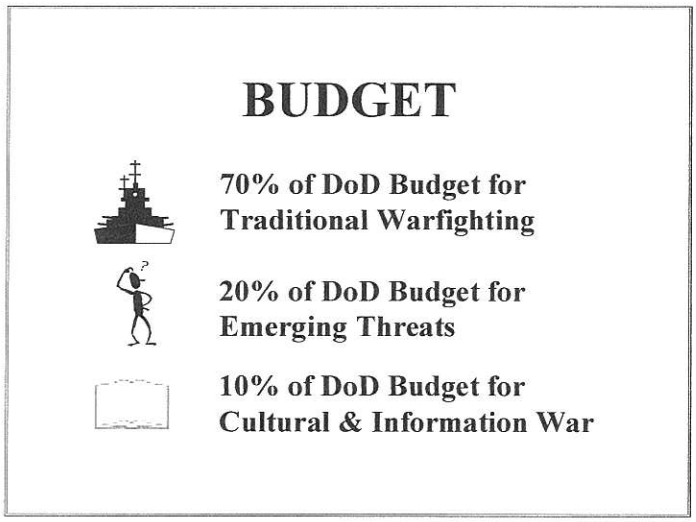

Figure 8. Leveraging the DoD Budget.

While remaining under the oversight of the armed services and national security committees, it is essential that additional funds be earmarked for emerging threats (for which a new sub-committee has fortuitously been formed this year on the Senate side) and for cultural and information war. The Emerging Threats oversight authorities in Congress will require some form of cross-over authorization authority with their counterparts on the Judiciary committees (to address special operations and transnational crime) and on the Foreign Affairs committees

(to address realignments toward information peacekeeping and assistance).

Reserve and Guard Implications.

The Reserve and National Guard forces that exist today are a vestige of the past, when **generic** manpower was the critical weak link in mobilization. Utilizing the Reserve and the National Guard was primarily about **bodies—**about **manpower** and being able to supplement the active duty forces. While that aspect remains, what has really become important about the Reserve and the Guard, at least conceptually, is their ability to "bank" special skills that need not be on active duty until they are actually needed—this is about **brainpower**.

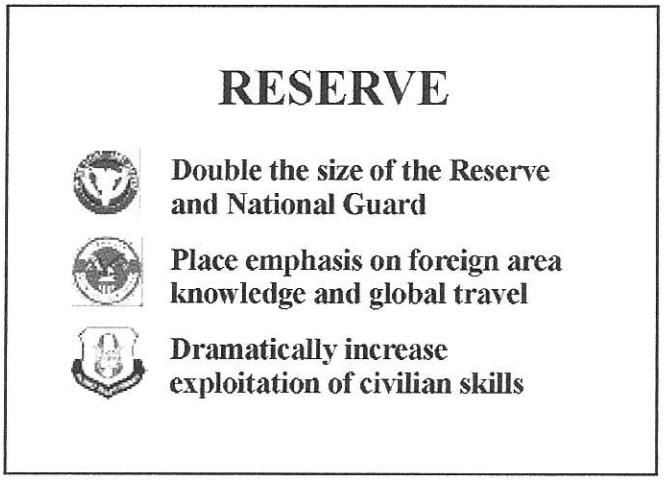

Figure 9. Leveraging Private Sector Through Reserve and Guard

Instead of fruitlessly attempting to train active duty personnel in specific foreign languages they are allowed to use for only one operational tour before returning to the normal career pattern, the United States should use the Reserve. We should create entire regiments dedicated to specific language groups (e.g., Arabic, Chinese, Russian), with each regiment having a battalion of intelligence

specialists, a battalion of military police, a battalion of engineers, and a battalion of judge advocates and public affairs specialists.

With such a regiment, it would be a simple matter to rotate each company within the battalion in sequence, and in this way provide for very high quality foreign language and foreign area support. Such a regimental organization could be "virtual" in that members could be located anywhere in the world, training together just once a year, but familiar with one another through collaboration tools and online exercises, and intimately familiar with their area of interest because of their civilian employment.

The National Guard could fruitfully consider a complete make-over in which it becomes the heart of Homeland Defense, with separate battalions or even brigades trained to support law enforcement, to carry out disaster relief, and to provide for electronic security and counterintelligence. The legal restrictions on the use of the military to carry out law enforcement duties within our borders are sound, but represent an old paradigm. Those elements of the National Guard assigned to law enforcement duties should in fact be a law enforcement reserve, not a military reserve, and should have all of the training, certification, and authority of a normal law enforcement officer.

The Reserve and the National Guard would also be excellent environments within which to test new roles and relationships, as well as new legal parameters, without interfering with our active duty readiness, and without detriment to the effectiveness of our active duty forces.

Private Sector Roles and Responsibilities.

The 21st century will see a transformation in the relationship between government and the private sector, between the military and commercial providers, between law enforcement and private security companies.

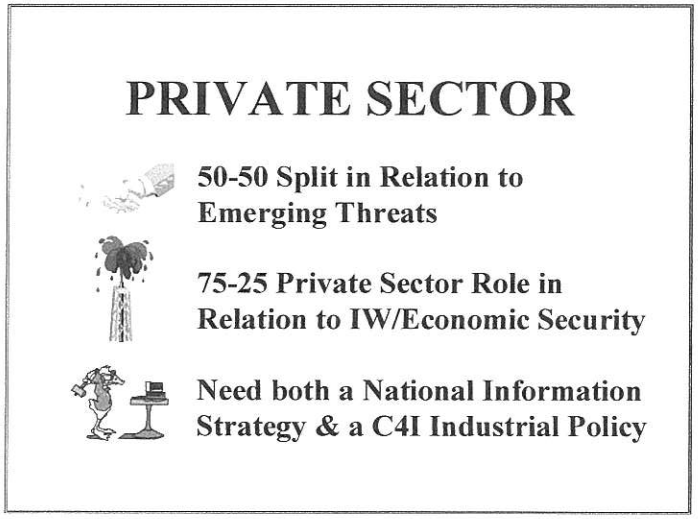

Figure 10. New Roles and Responsibilities for the Private Sector.

"Overt action" will replace "covert action" as the primary means of influencing emerging threat groups.[13] In combination with legislative incentives and insurance risk premiums as well as employee demands, multinational corporations will finally find that their best interests are served if they plan jointly with government for the achievement of selected national security objectives of mutual interest. A major task for the Emerging Threats Subcommittee in the Senate will be that of leading the discussion and definition of what these new roles and responsibilities for the private sector must be.

In relation to information warfare and economic security, it will be incumbent on Congress to pass "due diligence" legislation that places the major responsibility for self-protection on the private sector, while also requiring the communications and computing industries to live up to tough real-world standards for "safe computing."

Finally, both Congress and the Administration will have to come together to establish in carefully selected areas where consensus is achievable, both a national information strategy and a Command, Control, Communications, Computers, and Intelligence (C^4I) industrial policy. We

have neither a national information strategy today, nor an industrial policy. The National Information Infrastructure is primarily focused on connectivity and was originally a plan to provide five selected research centers with very high bandwidth—the plan was hijacked by the civil libertarians and became a popular initiative to wire schools and businesses into the Internet. At the same time, the U.S. Government historically eschews an "industrial policy" for fear of being tarred with the brush of government interference with business. In fact, the vulnerability of America to both electronic attack and global economic instability are so great that nothing less than a coherent collaborative effort between the government (both Federal and State) and the private sector (with the knowledge and the resources) will permit us to establish a national information strategy as it pertains to homeland defense and home-based aspects of both national security and national competitiveness.

Information Strategy.

Today's decisionmaker, from the president and the Secretary of Defense down to the most junior commander, lacks both a focused collection capability for obtaining all Relevant Information, and a reliable "all-source" analysis system able to fuse secret and non-secret sources into distilled, reliable and timely "intelligence."[14] The current staff process for any decisionmaker relies almost completely on a stream of "free" inputs received from counterpart bureaucracies, international organizations, and private sector parties pursuing their own agendas. At the same time, the narrowly focused secret or restricted steam of information is often afforded direct access to the decisionmaker without being subject to in-depth staff scrutiny and proper integration with unclassified official and external information. Functionally, today's staff process lacks the organization, knowledge, and funding necessary to methodically obtain information from specific international and other non-governmental organizations or

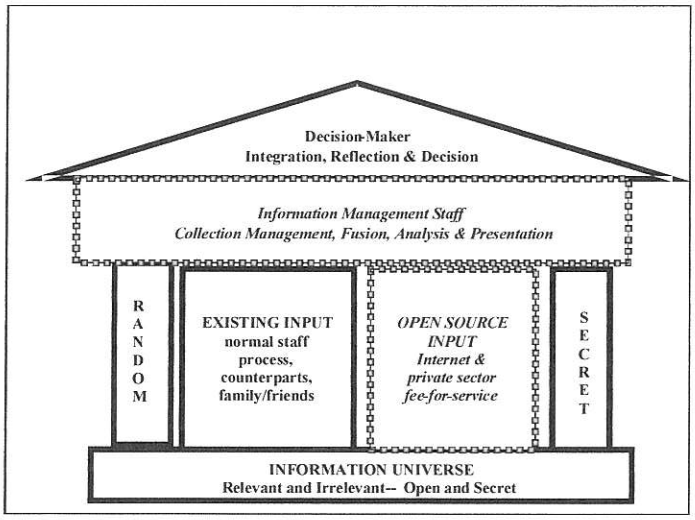

Figure 11. Enhancing Internal Capabilities Through Relevant Information.

to manage the collection of original information from external sources. Over-arching both these limitations, there is no top-level Relevant Information analysis staff organization that is able to provide the decisionmaker with filtered, fused and analyzed "all-source" decision-support. The major initiative in the early 21st century within defense must be the restoration of command responsibility for being properly informed, to include major procurement actions pertaining to open sources of information.

Changing Rules of the Game.

The United States has spent decades—a half-century—refining an information management system which assumes that

1. secret sources and methods are the heart of our national-level decision-support process;

2. leaders will decide and the people will follow; and

3. our most important decisions are "time-sensitive" with relatively obvious detail.

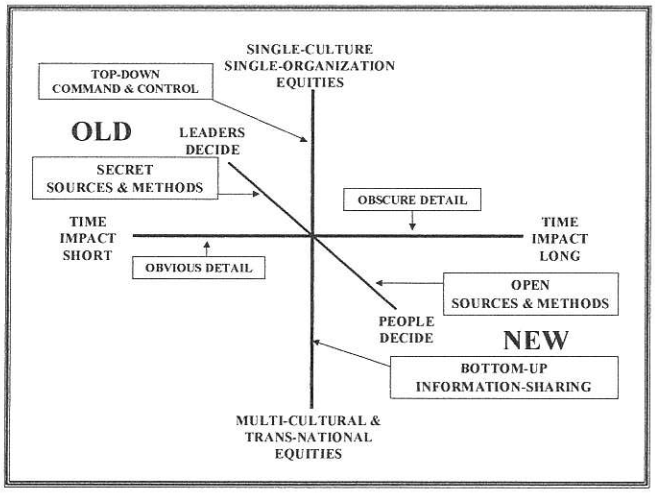

Figure 12. From "Control" to Consensus.

Our traditional construct is still applicable to many issues, but both our political environment and the information environment have turned many of our basic premises upside down. We are entering a century when the ability to master open sources—the vast flood of open sources in many languages, many mediums, many levels of detail—will be vital to public decisionmaking about very complex issues including the survival of several generations across several continents. Unfortunately, we have constrained our ability to confront the challenges of the day.

As Senator David L. Boren notes in his foreword to my book, *On Intelligence*, presidential policymaking in the future must pay much greater heed to cultural and psychological factors. Our decisions in the future must be made in partnership with non-governmental organizations, as they control the majority of the needed information and also have superior networks for achieving consensus within their chosen issue areas.[15]

What this really boils down to is a need to both think, and produce, intelligence in forms that can be shared with

domestic as well as international constituencies. We must, in other words, turn our own intelligence community on its head, and focus on creating a new and much enhanced community that embraces the private sector's mastery of open sources of intelligence, while refocusing our secret capabilities much more narrowly.

Building Blocks for Creating a "Smart Nation."

In the age of information, "warfare" and "national security" are at root about how a nation manages its intellectual resources. A nation's ability to discover, discriminate, distill, and digest "intelligence" is the core competency in the age of information.

Policy intelligence cannot and should not exist in isolation. To be truly effective in a networked world where the "butterfly effect" can have significant unanticipated consequences, policy intelligence needs to have four pillars: international intelligence that draws on military, coalition, law enforcement, and business as well as media sources; domestic intelligence that draws on legally and ethically available domestic sources of all kinds; strategic intelligence that deliberately draws out alternative scenarios and thinks unconventionally about both domestic and international issues; and integrative intelligence that makes sense of the other three in relation to both external threats and domestic imperatives.

The foundation for a "smart nation" is an educated citizenry. Indeed, a wise man once said that "a nation's best defense is an educated citizenry." A major aspect of any national information and intelligence strategy must be the development of architectures and protocols, including oversight standards, that nurture civic duty, educate citizens as to both the threats and opportunities facing America, and provide a means for individual citizens to contribute vital indications and warnings at every level of government.

Elements of a National Information Strategy.

Three specific elements of a national information strategy are recommended. None exists today, nor is any one of these three elements being seriously discussed at any level of government.

First, it is essential that a national strategy be devised for the digitization and preservation of content. Although our leaders have long understood that vast stores of knowledge were going to waste for lack of connectivity, the vaunted National Information Infrastructure (NII) does little to encourage the organization and enhancement of web-based knowledge. A wide variety of standards, as well as financial incentives, are required if we are to rapidly move dissertations, conference proceedings, and other mainstream publications to a web-based architecture that is properly indexed and also properly protected in terms of electronic copyright and electronic payment.

Second, it is essential that the process for developing standards for software be accelerated and also stabilized. A minimal standard for compound documents (integrated text and images) is required by law if we are to leverage the power of the Internet and the power of desktop capabilities across organizational lines. Security and inter-change standards are also required and they must be understandable by anyone with access to a computer. The current debate over Microsoft illustrates this problem perfectly—Microsoft's continued unwillingness to make its Application Program Interfaces (API) transparent and stable could be said—has been said by some—to have seriously undermined U.S. national security and national competitiveness.

Finally, we need a digital Marshall Plan as well as a digital New Deal. America lives in a glass house and is terribly vulnerable, not only to asymmetric attacks on its electronic infrastructure, but to self-generated crises caused by ignorance and a lack of global understanding. We

Figure 13. Recommended National Information Strategy.

must bring Africa, the Middle East, Asia, the Balkans, and Latin America into the 21st century, and do so in the grand manner that we evinced when saving Europe in the aftermath of World War II. At home, we must exert special efforts to empower every individual, whether schoolchild or adult with reading difficulties, so as to make our entire population, within a single generation, Internet-capable.

Elements of a DoD Information Strategy.

I have written elsewhere[16] about information peacekeeping as the purest form of war and about the central role that intelligence must play in the 21st century. It is vital for all of us to understand that in the Information Age, bytes are bullets, we are in a state of constant chaos and competition, and we require the total mobilization of all of the brain-power, all of the intellectual property, all of the information, that is in any way available for harnessing to the common good. In this era, the heart of national security and national defense lie in the domains of information and intelligence and not in the traditional domains of armed forces. DoD, however, must still take the lead.

This chapter suggests that DoD ask not what the president can do for DoD but rather ask what DoD can do for the president. The bottom line here is that only DoD has the resources—if managed wisely—to provide the president with the flexibility to create new methods for managing national security, and for funding new priorities that are unconventional in nature and span traditional departmental boundaries.

DoD must choose to pay the bill for this larger national construct—it must help pay the bill for a restructuring of the National Security Council; for the creation of a position of Secretary General for National Security; for the creation of four separate net assessment centers; and for the funding of modest but very valuable initiatives including a digital Marshall Plan and a digital New Deal.

DoD can set the example for how policy and operations will be managed in the 21st century by going virtual on its task forces and devising means for rapidly and readily including private sector experts—from all walks of life, all nations, with and without clearances, into its decisionmaking process.

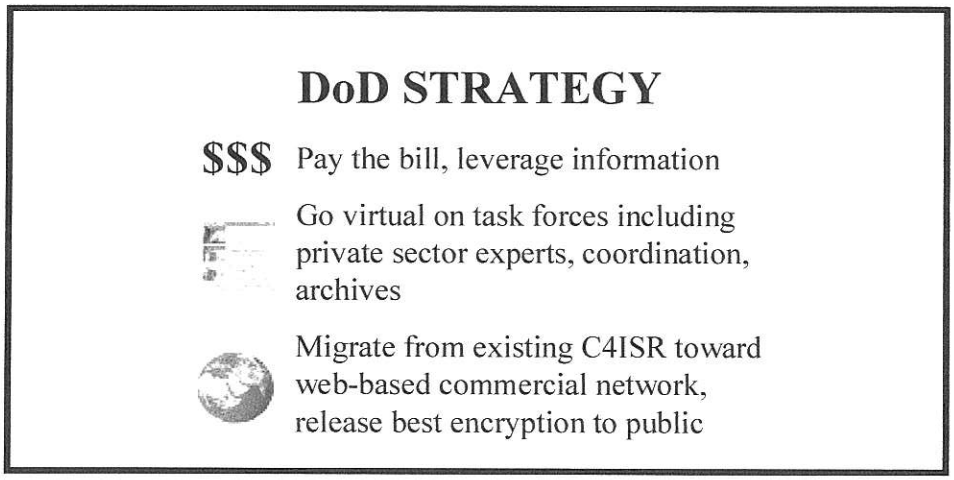

Figure 14. Recommended DoD Strategy.

At the same time, because this kind of global virtual architecture must of necessity be web-based, it is essential that DoD plan now for quickly migrating away from its existing Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C^4ISR) infrastructure. DoD must become the champion for permitting presidential-level encryption—the best that the National Security Agency is capable of devising—into the public domain, for the simple reason that in the 21st century, the president's most important counselors and sources of insight are going to be in the private sector, not within the U.S. Government. Only DoD can lead this radical migration.

Elsewhere, in the rapid expansion of NATO with its constantly increasing number of bi-lateral Partners for Peace (PfP), we see opportunities for new forms of regional intelligence concepts, doctrine, and architectures. The PfP can be best served by having NATO move away from the U.S.-dominated C4I infrastructure that is very secret and very expensive, and adopt instead an Internet-based architecture that anyone can join at whatever their level of computer and communications sophistication.

Also in Europe we see the forthcoming demise of the Western European Union (WEU) actually sparking a very robust discussion about the need for a European intelligence policy and regional European intelligence architectures. The WEU Satellite Centre at Torrejon, having proven its value, is likely to become the centerpiece of the first-ever regional intelligence community, where selected national and even U.S. capabilities are connected "virtually" to produce regional intelligence. The United Kingdom Open Source Information Centre; the Joint Analysis Center at Molesworth, and the German pilot project to mix civilian, military, and law enforcement intelligence specialists are all candidates for virtual integration to serve both Europe and NATO.

Virtual Reach.

Figure 15 describes this new approach to information sharing. Instead of relying on a single *President's Daily Brief* as the top-level intelligence document for each day, instead of relying on a tiny cadre of grossly over-worked members of the National Security Council staff, the president, and his principals in government, will have achieved a "virtual reach" that embraces and leverages all knowledge available throughout the government (and down to the state and local governments), all knowledge available throughout the nation, including the richest possible sources of knowledge in academia, the media, and the business community, and all knowledge available globally.

We have a long way to go before we can move within this virtual intelligence community with ease. New standards and understandings will have to be developed encompassing how we share information, how we compensate one another for shared information, how we pay for selected services, and how we authenticate individuals and organizations as sources of information. This is nothing short of a major global campaign to "make sense" across national, ethnic, class, and educational boundaries. Just as the world once had to devise fuel, rail, and highway standards to facilitate global commerce, so now must the world establish information exchange and information compensation standards.

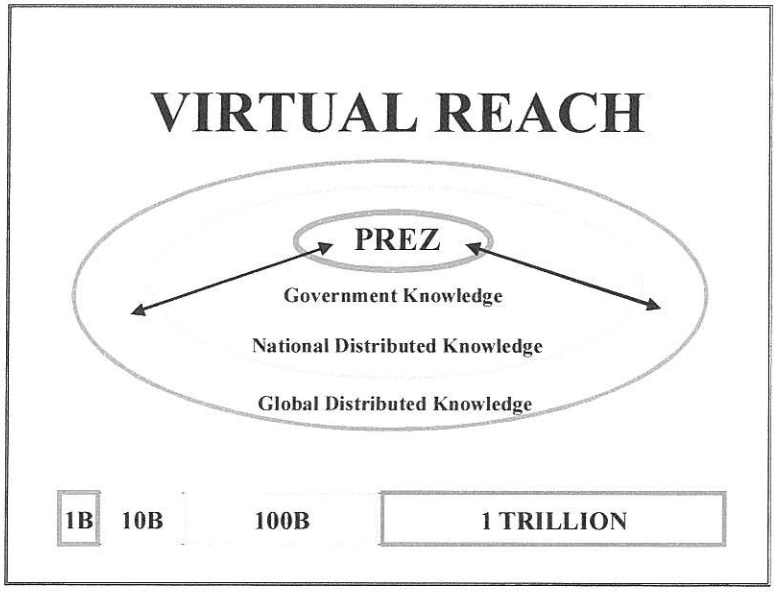

Figure 15. Creating the Virtual Intelligence Community.

Conclusion.

The conclusions to this study are straight-forward.

1. DoD leadership must empower the president—it will not work the other way around. DoD leadership, working in concert with its authorization and appropriations counterparts in the Senate and the House of Representatives, must come to a deliberate understanding of the world, of the need, and of the means by which to empower the president and restore coherence to U.S. national security policy making and operations.

2. DoD has the funds to enable full cooperation from both the Department of State and the Department of Justice. This entire program will cost no more than $3 billion a year—$1.5 billion for a national intelligence make-over that fully integrates open sources of intelligence into Federal decisionmaking—and $1.5 billion a year for a global digital Marshall Plan that has digital New Deal elements here at home.

3. There is no need to physically restructure the government. Speaking in very practical terms, the Secretary General for National Security and all of the new elements proposed for the National Security Council can be housed in the South Central campus near the Department of State and recently vacated by the Central Intelligence Agency.

4. There will need to be a Presidential Decision Memorandum and consensus on the Hill in order to achieve legislation with the necessary statutory authority for both the new Secretary General for National Security, and several of the president's principal staff including the Director General for National Policy, Director General for National Intelligence, the Director General for Global Strategy, and the Director General for National Research.

The United States is at a juncture where the president can neither direct nor persuade. Presidential leadership in national security policymaking requires a startling leap forward, a leap that can only be financed and bureaucratically enabled by the Department of Defense. It will take a small group of like-minded leaders, but if such a group can be put into place, the rest of the department, and hence the rest of the government, will follow. Only in this way can cohesion and continuity be restored to presidential leadership and national security policymaking.

ENDNOTES - CHAPTER 12

1. The original version of this paper is at *www.oss.net/Papers/white/S99Paper.doc*. A published version is at *www.defensdaily.com/reports/securpolicy1099.htm*.

2. "TAKEDOWN: The Asymmetric Threat to the Nation," *Defense Daily Network,* December 1998, at *www.defensedaily.com/reports/takedown.htm*.

3. Dr. James Schlesinger said this to the Senate Committee on the Budget, February 24, 1999. The complete text of his remarks is reprinted in *Colloquy*, April 1999.

4. The political science literature makes reference to a 6-year period as the norm for change in organizations that desire change. Senator Daniel Patrick Moynihan (D-NY), writing in *Miles to Go: A Personal History of Social Policy*, Cambridge, MA: Harvard University Press, 1997, writes of how it takes 25 years to effect significant change in U.S. policies and the organizations and spending patterns that reflect those policies.

5. Mich E. Kabay, *The NCSA Guide to Enterprise Security: Protecting Information Assets*, New York: McGraw-Hill, 1996, Chapter 1, Figure 1, p. 11. The figure in the book is superseded by this information, provided by Dr. Kabay in personal communications to Robert Steele, OSS CEO, March 12, 1998.

6. The Clinton administration National Security Council has the following elements, in this order of priority:

Office of the National Security Advisor
Executive Secretary
African Affairs
Asian Affairs
Central and Eastern Europe
Defense Policy and Arms Control
Democracy, Human Rights and Humanitarian Affairs
Environmental Affairs
European Affairs
Global Issues and Multilateral Affairs
Intelligence Programs
Inter-American Affairs

This is actually a pretty good organization for dealing with the spectrum of defense and diplomatic issues. It can be functionally improved, especially in relation to transnational criminal and financial issues, cultural, migration and health issues, and science & technology issues. One alternative treatment of how best to improve national security policymaking in relation to home defense, finance and trade, and science and technology is provided in Stephen A. Cambone, *A New Structure for National Security Policy Planning,* Washington, DC: Center for Strategic and International Studies, 1998.

7. Richard E. Neustadt and Ernest R. May, *Thinking in Time: The Uses of History for Decision Makers* New York: Free Press, 1988, provide a valuable study of how different times provide different measures and different perspectives from which to address the same facts. They suggest these measures and perspectives should be operationalized for the White House within the global strategy unit. This same unit should also be conscious of the full range of works on clashing civilizations, cultural imperialism, religious filters, and so on. If the National Intelligence Council is the integrator of "real world" information, then

the global strategy unit must be the integrator of the intangible factors and the "wild card" aspects that tend to be set aside by the day-to-day analysts and their managers.

8. David M. Abshire, *Preventing World War III: A Realistic Grand Strategy*, New York: Harper & Row, 1988.

9. For a complete critique of our existing intelligence community and detailed recommendations on where we need to go, see *On Intelligence: Spies and Secrecy in an Open World*, AFCEA International Press, May 2000. With a foreword by Senator David L. Boren (former Chairman of the Senate Select Committee on Intelligence) and supporting blurbs from The Honorable Dick Kerr, former Deputy Director of Central Intelligence as well as several European flag officers, the book includes detailed recommendations for dramatically enlarging the scope and substantially changing the nature of the U.S. Intelligence Community. With a 50-page annotated bibliography that integrates Silicon Valley, Internet, management, and hacking books with the more traditional literature; a 62-page index; and 30 pages of proposed legislation, the National Security Act of 2001, this is a basic reference work on intelligence. Available directly from *www.amazon.com*.

10. *On Intelligence*, endnote 11, Chapter 8.

11. *Ibid.*, endnote 11, Chapter 12. Harlan Cleveland, *The Knowledge Executive: Leadership in an Information Society*, New York: E.P. Dutton, 1985, makes a compelling case for precisely this kind of "higher education" for policymakers.

12. OODA Loop: Devised by Col John Boyd, "Orient, Observe, Decide, Act." As Bill Gates has noted in his latest book, *Business @ The Speed of Thought*, New York: Time Warner, 1999, the chief characteristic of the 21st century is going to be "velocity." This point was made in the 1980s by Brigadier Simpkin in his book, *Race to the Swift: Thoughts on 21st Century Warfare*, Washington, DC: Brassey's, 1985.

13. In the early 1990s David Ignatius, then editor of the Outlook section of *The Washington Post*, wrote a very provocative piece on how overt groups were proving much more effective than covert campaigns to foster democracy and achieve other worthy goals.

14. The conventional understanding of "intelligence" as information that is inherently classified is incorrect. Data is the raw print, signal, or image. Information is data that has been collated into a

generically useful product that is generally broadcast. Both the *New York Times* and most of what is now called "intelligence" are actually unclassified or classified *information*. **Intelligence** is information that has been deliberately discovered, discriminated, distilled, and delivered to a decisionmaker in order to answer a specific question. Most intelligence is **not** classified.

15. Jessica Matthews makes this argument in "Power Shift," *Foreign Affairs,* January-February 1997.

16. *On Intelligence*, endnote 11, Chapter 10.

"Presidential Leadership and National Security Policymaking", in Douglas T. Stuart (ed.), *Organizing for National Security* (Strategic Studies Institute, U.S. Army War College, 2000), pp. 245-282.