Secretary of Defense
Strategic Studies Group IV

1999 Final Report

Premises for Policy:
Maintaining Military Superiority
In
The 21st Century

#962

Contents

Foreword

The Secretary of Defense Strategic Studies Group [SSG] was established on July 5, 1995 by Secretary of Defense William Perry. The purpose of the SSG is to build a cadre of future military leaders who understand and can address the broad strategic management issues that will face the Department of Defense in the years ahead. Officers were selected competitively from each Service for their high flag- and general-officer potential, to spend 10 months focused on an issue selected by the Secretary of Defense.

SSG IV was convened on July 1, 1998. It was tasked by the Deputy Secretary of Defense to respond to this challenge:

> In an era of an increasingly globalized U.S. economy, and marked by increased availability and global flows of information, what do we need to protect and preserve, to sustain U.S. military advantage in the early 21st century?

SSG IV responded with a series of "premises for policy"—the independent and collective judgments of military officers who have distinguished themselves in a wide variety of operational command and staff positions. These premises were offered as a basis, with supporting rationale, for the Department of Defense to use in developing policy.

Their report includes premises for policy covering:

- Information and technology
- People
- Experimentation
- Space
- National-level initiatives

SSG IV has raised a number of issues worthy of consideration and possible action by senior management within the Office of the Secretary of Defense, the Joint Staff and the Services. I value the insights and perspectives of SSG IV's report and commend it to you.

A.W. MARSHALL
Director, Office of Net Assessment

Executive Summary

The Secretary of Defense Strategic Studies Group IV (SSG IV) was formed on 1 July 1998. The Deputy Secretary of Defense has tasked SSG IV to help focus his thinking about potential policy solutions to this challenge:

> In an era of an increasingly globalized U. S. economy, and marked by increased availability and global flows of information, what do we need to protect, preserve, and sustain U.S. military advantage in the early 21st century?

SSG IV investigated the protection of technologies relevant to sustained military superiority, and the protection of information and the systems that contain and promulgate information.

In an era when:

- Industry is globalized,
- The U.S. lead in militarily relevant technology may be shrinking, or may no longer exist at all,
- The U.S. military relies increasingly upon commercial technologies and products, and
- Product-introduction cycles grow increasingly shorter

DoD must be selective in the technologies it chooses to protect.

The best interests of the U.S. economy demand that we protect only the most critical elements, while creating the greatest possible competitive maneuver area for American business in the global marketplace. A strong U.S. economy forms the foundation of a strong national-security structure.

As we move into the 21st century, increasing reliance on both information and information systems will require increasing levels of protection. The ability to create, transmit, and use classified and unclassified-but-sensitive information effectively will be critical to attaining rapid dominance on the battlefield and any other military objective. Therefore, the ultimate goal of information protection must be to ensure reliable continuity of operations.

The essence of this report is "Premises for Policy"—relating to the protection of information and information systems. SSG IV also has added sections on people, experimentation, space, and other national-level defense issues. In the course of interviewing leaders in government, industry, and academia, SSG IV gathered many insightful thoughts regarding military superiority in the future. The best of these ideas—as well as the SSG IV's mining of its own ideas—are captured in all of the "Premises for Policy." It must be emphasized that these premises are merely starting points to help the Secretary of Defense focus his thinking on develop maintain military advantage in the 21st century. Further effort will be required to develop effective DoD policies based on these premises.

Introduction

The Deputy Secretary of Defense has tasked SSG IV to examine and recommend policy solutions to this question:

> In an era of an increasingly globalized U. S. economy, and marked by increased availability and global flows of information, what do we need to protect, preserve, and sustain U.S. military advantage in the early 21st century?

The SSG IV's study has focused on the protection of technologies relevant to sustained military superiority, and protection of information and the systems that contain and promulgate information. Similarly, the Defense Science Board and the Defense Policy Board have been asked by the Secretary and Deputy Secretary of Defense to examine from their special perspectives what the Department might do to sustain military superiority in an era of economic globalization and increasing information flow. SSG IV has conducted a series of detailed discussions with senior administration policymakers, former Department of Defense officials, senior representatives of the Defense industry and other U.S.-based multinational and global business enterprises, and several Unified Commanders-in-Chief. SSG IV has devised policy premises for Department of Defense action in both these areas, briefing them to the Deputy Secretary of Defense, other key officials in the Office of the Secretary of Defense, the Joint Staff, and the Service Chiefs.

SSG IV was comprised of:

Colonel (sel) Mark L. Broin, USMC

Captain Robert D. Maslowsky, USN

Captain James F. McEntire, USCG

Colonel Ronald R. Reichelderfer, USA

Captain Paul J. Ryan, USN

Colonel James J. Westlake, USAF

Lieutenant Colonel Kevin E. Williams, USAF

SSG IV's Approach to the Tasking

➢ Methodology

In considering the scope of technology and information protection, SSG IV has examined them in their strategic context. Therefore, SSG IV's study has proceeded along four parallel tracks:

- Craft a view of the current and future global security environment.
- Develop a simple but effective conceptual model of overall military capability.
- Consider what the U.S. military must be able to do in the years ahead.
- Devise concepts and institutional approaches for protection.

➢ Security Environment and U.S. Defense Policy Context

The international security context in which the Department of Defense operates on the eve of the 21st century differs fundamentally from that of the Cold War era. Today, the United States has no single, dominant threat for its military to face. Rather, our nation must use its Cold War-legacy assets to further military and national-security strategies that postulate a world essentially at peace—albeit one in which small-scale and regional conflict have become more possible. National interests are articulated in the President's 1998 National Security Strategy document, which states that the U.S. military is sized to prevail in two nearly simultaneous major theater wars, or one major theater war while conducting multiple smaller-scale contingency and engagement operations in other theaters.

The U.S. economy is expected to remain strong, in light of lowered trade barriers and an increasing flow of global capital to areas of greatest opportunity or least risk. U.S. businesses have adapted well to the rigors of a global marketplace, and remain the prime force as the engine of global economic growth. The Internet continues its phenomenal growth, and its impact on the ways organizations conduct business still is evolving rapidly. Computing capacity and capability continue to grow—today's desktop computer has the capability of yesterday's mainframe—and tomorrow's personal computer will be even more capable. Economic rationalization continues on a global scale, despite the occasional discontinuities caused by severe downturns of some national economies. Successful businesses in the United States have conformed to the realities of global competition by focusing only on areas that yield sustained competitive advantage, while outsourcing all other aspects. In manufacturing and software development firms, this often means that manufacturing or code-writing operations are distributed globally, not simply contracted to other firms indigenous to the United States.

The Chairman of the Joint Chiefs of Staff has articulated a vision of required future U.S. military capabilities in *Joint Vision 2010*. Each of the Services has created a vision of its own intended support of the *JV 2010* concepts. The responsibility for joint experimentation has been assigned to the Commander-in-Chief, U.S. Atlantic Command, who is executing that mission in concert with each Service's doctrinal development and war-fighting laboratory establishment. One particular aspect of joint and service policy is relevant to SSG IV's work: Future conflicts involving the U.S. military are likely to be conducted in a coalition framework. Nevertheless, the U.S. military must be sized to prevail unilaterally.

As a consequence of finite resources and the need to maintain overall current military readiness at high levels, the Department of Defense acquisition strategy has become more reliant on commercial, off-the-shelf technology. The Defense sector of U.S. industry has adapted to this reality and conducted a series of mergers to enhance economies of scale, while that sector of European industry is in the initial stages of consolidation.

Difficult policy issues for the United States are created by the potential trans-Atlantic mergers and acquisitions among the Department of Defense's traditional domestic industrial suppliers. These were not addressed directly by SSG IV, but the knowledge of these issues and their implications were central in our thinking. Annex A offers criteria and processes that could perhaps be applied to such issues.

Another complex issue in the information-protection arena arises in identifying the information that must be protected. Obviously, certain types of information—such as classified information and information subject to the Privacy Act[1] and other such laws—should be protected. Also, sensitive government information—not necessarily national security information *per se*—should be protected as well. SSG IV did not undertake a review of the Executive Order[2] governing the classification and protection of national security information, because that remains outside the scope of its study.

Presidential Decision Directive 63, addressing the protection of the nation's critical infrastructure, contains examples of unclassified-but-sensitive information and information systems. The Department of Defense depends on several critical national-information infrastructures it does not own; is designated as lead agent for the National Communications System; and is responsible for coordinating protection plans with other government agencies and private sector owners of this infrastructure.

It is against this backdrop—with substantial global engagement by forward-deployed forces; without a peer competitor, but concerned about asymmetric threats; and operating in an environment punctuated by periodic regional conflict—that SSG IV conducted its study of technology and information policy.

[1] P.L 93-579 (5 U.S.C. 552a, et. Seq.)
[2] E.O. 12598 dated 17 April 1995; subject: "Classified National Security Information"

➢ Conceptual Model for Military Capability

Overall, military capability can be considered as a function of the interaction between several factors:

- *People*
- *Training*
- *Equipment*
- *Doctrine and Organization*
- *Experimentation*

Information flow, and the resulting creation and application of knowledge, pervades the entire model. Other factors—such as resource levels, capital investment allocations, and the National will—are critical enablers but are not integrated into the model.

This model can be applied to single-service, joint, or combined forces across the full range of conflict. It does not necessarily encompass non-traditional combinations of interagency capability, but it allows for an expanded interagency role in national security. Newer forms of warfare will require different combinations of skills and organizations.

➢ Imperatives for Future U.S. Military Capability

The U.S. military must be able to perform certain critical tasks to achieve whatever objectives the National Command Authority might specify. SSG IV believes that the National Security Strategy and National Military Strategy—both current and future—will require the U.S. military to:

- Project power anywhere and anytime, as dictated by the national interest.
- Create, collect, promulgate, and store information, developing knowledge adequate to conduct successful military operations.
- Create and amass effects—destructive, psychological, or coercive by any other means—powerful enough to attain the desired result.
- Counter the effects of weapons of mass destruction or weapons of mass disruption used by any adversary to blunt or negate U.S. military capability.
- Prevail across the full range of conflict.

Although lower-intensity conflicts will present the most frequent scenarios, the U.S. military also must be prepared for worst-case scenarios. A major theater war must retain the most intense focus of the U.S. armed forces, because it presents the most difficult of military tasks.

➢ **Concepts of Protection**

The goal of technological or information security is to guarantee freedom of action—and to ensure that when the Nation does act with military forces, those forces will be able to attain objectives by means of strategic, operational, and tactical surprise. Thus, ensurance of result is the fundamental military objective of security. Therefore, the philosophical underpinnings of any scheme of protection for technology, information, or information systems should be ensurance rather than simply that of information denial, or of making systems assault-proof.

➢ **Summary**

SSG IV's focus has been on protection of technologies relevant to sustained military superiority, and protection of information and the systems that contain and promulgate information.

In an era when

- Industry is globalized,
- The U.S. lead in militarily relevant technology may be shrinking, or may no longer exist at all,
- The U.S. military relies increasingly upon commercial technologies and products, and
- Product introduction cycles grow increasingly shorter,

DoD must be selective in the technologies it chooses to protect.

The best interests of the U.S. economy demand that we protect the most critical elements, while creating the greatest possible competitive maneuver area for American business in the global marketplace. A strong U.S. economy forms the foundation of a strong national security structure.

As we move into the 21st century, increasing reliance on both information and information systems will require increasing levels of protection. The ability to create, transmit, and use classified and unclassified-but-sensitive information effectively will be critical to rapid dominance on the battlefield or any other military objective. Therefore, the ultimate goal of information protection must be to ensure continuity of operations. This is a vital element of the military dominance envisioned in joint and service visions.

The remainder of this report contains premises for policy related to protecting information and information systems. SSG IV also has included sections on people, experimentation, space, and other national-level defense issues. One of the most rewarding aspects of the SSG experience has been the access to a wide variety of leaders in government, industry, and academia. In the course of interviewing these leaders, SSG IV obtained many new insights related to military superiority in the future. The best of these thoughts and ideas, as well as SSG IV's mining of its own ideas, are captured in all of the "Premises for Policy" section that follows. It must be emphasized that these premises are merely starting points to help the Secretary of Defense focus his thinking on maintaining military advantage in the next century. Further effort will be needed to develop effective DoD policies from these premises.

Finally, Annex A is a detailed description of a proposed new process for evaluating the critical technologies that need to be protected. If nothing else, it should provide a basis for analysis and debate about ways to best identify the technologies that need protection.

Premises for Policy

The results of SSG IV's research are summarized in a series of premises. Our task was not to write policy, but to provide the bases upon which DoD policymakers could craft policies in key areas of concern. The following premises are provided for consideration:

➢ Information and Technology

We need new criteria and new processes to determine which technologies, skills, and intellectual capital need protection.

Premise: *That DoD lacks a coherent, institutionalized process by which it can rationally identify existing and emerging technologies and operational concepts that have the potential to help sustain global military dominance.* (See Annex A).

Premise: *That system integration process is a key U.S. strength; therefore, foreign access to technology and intellectual capital that support integration capabilities needs to be restricted.*

Although the U.S. does not lead in all technology areas, it has a unique ability to combine individual technologies or systems of technologies into larger systems. How well we field integrated systems ultimately will determine U.S. military advantage. Since technology diffusion cannot be prevented over time, leadership in system integration capabilities can offset a potential adversary's unique technological advantages. Attaining the primary military advantage of system integration requires cultural and educational qualities underpinning industry's—and the military's—integration ability to be identified, nurtured, and protected.

Premise: *That diffusion of discrete technologies is happening; therefore, we must protect only U.S. unique technologies; sell technologies to establish market leadership and cultivate dependencies; and pursue and embrace leading foreign technologies.* (See Annex A.)

Premise: *That technology sharing policy should promote the development of those future power centers the U.S. government wants to cultivate, not just historical allies.*

The Department of Defense has strong historical ties to European allies but—looking to the 21st century—it may see other areas of the world that have the potential of affecting vital U.S. interests. We should not downplay the importance of traditional alliances, but it is necessary to look to the future and develop cooperative development programs in regions that may produce potential new centers of power or long-term threats to U.S. interests.

Premise: *That commercial-off-the-shelf (COTS) products will not satisfy all military technology needs; a unique military technology base (e.g., antisubmarine warfare,*

reactive armor, stealth/counter stealth) will remain necessary and must be protected against emulation and (possibly) those seeking asymmetric advantages.

Although there may be ways to use enabling COTS technology and commercial manufacturing systems, unique military technology will still be required to maintain U.S. military advantage. Identifying, developing, and protecting these technologies requires continual assessment of emerging technologies, those with promise of providing the U.S. military with a clear advantage over potential adversaries. (See Annex A.) We must ensure our ability to produce unique military technologies by protecting both research and industrial bases needed to develop such technologies.

Premise: *That DoD-sanctioned international technology exchange mechanisms created in 1963[3] (i.e., the more than 1,000 Defense Data Exchange Agreements or U.S. lab-to-foreign military lab cooperative arrangements with 27 countries) should be revised into a single set of policy objectives based on a new security environment.*

There is no apparent relationship between the Militarily Critical Technology List (MCTL) and Data Exchange Agreements—which persist, based on outdated Cold War-era assumptions. DoD should review comprehensively and redraft all policies and DoD regulations governing departmental and contractor-generated information and technology-exchange agreements. The review should ensure that the underlying objective of each agreement is predicated on a fresh policy review, based on post-Cold War strategies and alliances.

How to provide needed protection

Premise: *That DoD needs to seek enabling legislation—comparable to existing policy with regard to attacks by traditional weapons—to improve our ability to defend against information attacks.*

At present, national policy and military doctrine are well-defined with respect to the use of DoD assets in event of nuclear, biological, chemical, or conventional attack. Nevertheless, policy and doctrine are lacking for DoD response to attacks on DoD information systems, or other critical national infrastructure. The prospect of cyber-retaliation raises significant policy and legal questions. Where is the proper transition point between peacetime and wartime rules of engagement? What is the doctrine for response, and how such responses should be structured for malicious attacks as opposed to overt cyber-hostilities? How do we respond to domestic attackers vís-à-vís foreign ones? What is the shared role of law enforcement and DoD? Because of today's reliance on passive defense, unsuccessful attacks on DoD information systems cause no sanction to accrue to an attacker. DoD must forcefully advocate clearly defined national policy and military/law enforcement rules of engagement for cyber attacks against DoD, government, and critical, privately owned national infrastructure.

[3] DODINST 2015.4 (now is undergoing revision).

Premise: *That DoD acquisition policy must include security considerations up front in all information systems acquisition.*

DoD is a leader in defining and requiring security for network systems.[4] With interconnected and interdependent information systems, information ensurance must be a major concern within the U.S. government as well as the private sector. It is far less expensive to design security features into information technology hardware and software applications up front (some cost-avoidance estimates show a ratio of 10:1) than it is to overlay it after initial development. DoD should require the computer hardware and software industry to build security features into their products to protect against inadvertent and malicious network and data intrusions.

Premise: *That DoD must establish policy to better enforce network interoperability and transmission security, and establish standards for non-DoD access.*

To date, DoD has been unable to implement a common department-wide infrastructure to facilitate interoperability among all DoD networks. Performance-Based Standards must be established, implemented, and measured for connectivity (secure and unclassified) among all Service and DoD agencies, and for third-party system integrity[5]. These standards both must absorb future changes in technology and must permit the Services to procure highest value within established guidelines. Achieving interoperability requires strong top-down leadership with the responsibility and authority to implement DoD-wide standards across organizational boundaries.[6]

Qualities of better information-protection strategy

Premise: *That efficient and effective DoD security requires stronger personal access as well as a single, DoD authorization system.*

DoD's present system of network authorization is weak and restrictive. DoD must incorporate a new physical element, in addition to its present mental element (Pin number), to form a stronger, more flexible personal-identification system that—when coupled with secure transmission links—will permit positive ID from any DoD workstation. Several leading network companies are investigating the development of "universal data base authorization systems".[7] These systems permit multiple levels of authorization company-wide, and at the same time are flexible enough to adjust to new

[4] Banking and financial sectors, as well as network providers are other industrial leaders in the network security field.

[5] SSG IV observed two excellent examples of implementing broad guidelines over a diverse multi-unit organization that have successfully achieved organizational interoperability: CITIGroup and Lockheed/Martin. CITIGroup also established "metrics" to see how well the corporation diverse units are doing.

[6] "Realizing the Potential for C4I: Fundamental Challenges" (Washington: National Research Council, March 1999), ES-5

[7] SSG IV was very impressed with the system-wide security architecture concepts under development at CISCO Systems and CITIGroup.

technologies or system-wide authorization policy changes. If DoD were to implement the new personal identification system—coupled with the soon-to-be-implemented public key infrastructure (PKI) procedures, secure encryption links and a universal data base authorization system—DoD networks can be secure, flexible and well positioned to accommodate future security challenges.

Premise: *That DoD is forgoing a major opportunity to shape industry security and performance capabilities to its advantage by not consolidating its software, hardware, and security requirements.*

As a national leader in security, DoD must set the design standards for others. This can be accomplished if DoD consolidated all its requirements for networks, software, and hardware. Such consolidation would give DoD increased leverage over commercial suppliers. For example, although DoD accounts for only 1% of Microsoft's business, it is its largest single customer. In addition, many private-sector purchasers without the scale of DoD would readily use products designed to meet DoD security standards. Like interoperability, establishing common standards requires strong, top-down leadership with the responsibility and authority to cross organizational boundaries.

Premise: *That the Chief Information Officer (CIO) and the Chief Information Assurance Officer (CIAO) should be independent and equal within the organization, to provide the proper balance between networking information and protecting information.*

At present, DoD places the head of information security under the Chief Information Officer. Most major corporations separate these functions to encourage a creative tension between information providers and protectors. The CIO is responsible for integration, acquisition, interoperability and attaining the highest efficiency and best value for DoD; the CIAO is responsible for systems availability, identification and authentication, confidentiality, non-repudiation and data integrity. These equities sometimes can conflict, so the proper balance between convenient interoperability and security must be reached. This balance is best accomplished by ensuring the CIO and CIAO are independent with equal access to DoD leadership. It then becomes the responsibility of DoD leadership to adjudicate issues of risk management, as it pertains to cost and timeliness versus security.

Premise: *That systematic vulnerability assessments are necessary not only for information systems but also across all DoD technological acquisitions.*

Short of war, the most effective method of vulnerability assessment for DoD technologies, information systems, and operational concepts is to apply broadly the "red team" assessment process. To be effective, this assessment process should not be limited to any one aspect or area of DoD, but also applied to new operational concepts, current doctrine, information systems, emerging technologies, and systems of systems. This process needs unfettered access, the ability to think like the nation's potential adversaries, and—most important—independence from the organizations and processes that develop, acquire, or implement technology, operational concepts, or information systems. The strength of wide-ranging, independent assessment teams composed of warfighters, so-called "ethical hackers," logisticians, and intelligence personnel lies in their ability to expose symmetric and asymmetric vulnerabilities, and aid in their elimination or mitigation. This assessment organization should rotate its members regularly so their skills, outlook, and experience have the widest impact on the Services.

Premise: *That validating the integrity of COTS software is difficult and in some cases impossible to do with current technology; therefore, DoD needs to pursue both government-off-the-shelf (GOTS) and enabling technology, to perform certification tasks to ensure the integrity of critical systems.*

As the DoD becomes more dependent on information technology, it becomes more dependent on COTS software products. DoD's challenge thus is to ensure that these products will perform predictably under strenuous conditions and that they will not be susceptible to security breaches. The sheer complexity of some COTS software products widely used in the DoD, such as Windows NT with tens of millions of lines of code, makes it virtually impossible to validate its suitability and security.[8] Furthermore, U.S. companies are increasingly outsourcing some COTS software production to non-U.S. entities.[9] DoD should fund and encourage the development of cost-effective tools to automate the validation of COTS software integrity, and pursue "government-off-the-shelf" (GOTS) solutions for mission critical software.

---

[8] Even Microsoft's managers were unable to detect that its software programmers had inserted "Easter Eggs" into its "Microsoft Office" suite of applications. The Easter Eggs are hidden sections of code contained within the application that are activated when the user enters a unique sequence of key strokes. The known Easter Eggs contained within the Microsoft Office products are believed to be harmless. If this "harmless" code can get by the software-quality and configuration control processes at Microsoft, it is easily conceivable that harmful code could get embedded in its products. Interestingly, the DoD response to the discovery of the extraneous code was to press Microsoft for a partial refund for the price it had paid for its hundreds of thousands of copies of Microsoft Office. This was based on the argument that the DoD should not have to pay for the time spent by the rogue programmers in creating the Easter Eggs.

[9] There is clear evidence that some software written in foreign countries contains code designed to compromise the security of the system the code is written to support. In some cases, this malicious code was discovered only after security breaches had already occurred.

Personnel and system protection

Premise: *That because the greatest threat to DoD's information system is the insider, we must: institute user profiling; establish a Personnel Reliability Program (PRP)-like program or use Two Person Integrity (TPI) when appropriate for critical systems; standardize the system administrator field; and mandate data storage encryption.*

Recent press coverage on information security has focused on external threats to computer networks—individual hackers or organized attacks sponsored by foreign nations. But the greater threat for network security is from an internal source—a disgruntled employee or someone susceptible to bribery.[10] There are four measures that can be applied to reduce this threat. They are:

Profile User. Databases store each user's normal activities, characterized by the type of work, access authorizations, and who is usually being interacted with. When a user's activities deviate from the profile thus built, an authorized individual is automatically alerted.[11] It is then up to that individual supervisor or other authorized person to decide if any intervention should take place.[12]

Use a Personnel Reliability Program-like program, or a two-person control mechanism for critical systems. Usually, a single person (the system administrator) has access to, and the ability to change, critically sensitive network security controls such as passwords and user accounts. Authority to access and alter selected critical functions should be subject to two-person control or redundant independent inputs.

Standardize the system-administrator career field. At present, system administrators are currently a weak link in network security. Adoption of networks throughout the Services was not accompanied by designated, funded personnel allocations for system or network administration. The system administrator is a security necessity for daily network maintenance and operation, but that function most often is assigned on an *ad hoc* basis from existing personnel authorizations. Several companies have identified this as a significant security issue and have established standardized training programs and career paths for this entry-level task.[13]

Mandate data storage encryption. Much of DoD's network-security architecture is based on a layered, defense-in-depth concept. Layering is designed to stop unauthorized individuals from gaining access to the network or system. This is the "crunch." On the other hand, once inside the network the attacker is free to search through the system to

---

[10] SSG IV found an overwhelming consensus among government and industry officials alike, that the greatest threat to computer network security is from inside the organization—such as disgruntled employees.

[11] This is essentially what credit card companies use today to detect unauthorized use—e.g., a stolen card.

[12] Several large diverse companies current employ this system on their company-wide networks (Lockheed/Martin, CITIGroup, Raytheon)

[13] This issue is also addressed in "Realizing the Potential for C4I: Fundamental Challenges," (Washington: National Research Council, March 1999), ES-13. This study recommended that the DoD provide competitive rewards, professional challenge, development, and recognition for this career area.

find files of interest. This defensive architecture is described metaphorically as, "crunchy on the outside, soft on the inside." Mandating the encryption of data files, either by static encryption of raw data or by encryption at the entry and exit ports, will reduce the "softness" of a network and strengthen DoD's information-security posture.[14]

Premise: *That existing security procedures are valid and essential but must be rigorously applied to alter the current cyber mind-set toward openness while operating on networks.*

DoD has become a networked organization and more reliant on the Internet, but its established security procedures and practices have been truly enforced only after they have been violated. An increased emphasis on established security procedures and practices, at every level of DoD, is needed. A network information security culture is required. Instilling attribution and accountability in the network itself will go far toward enhancing network security. Top-level leadership must promote information ensurance as an important cultural value to the same extent that protection of classified information has been.

Premise: *That since training and awareness are essential elements of information security, a common, mandatory, and recurring DoD-wide training program is required.*

Today in industry, there is a strong trend toward centralized information-system training programs. Many are executed monthly, others quarterly. Most cover a one-year cycle, and are continually refreshed with the latest lessons learned. Each business unit has the latitude to add unit unique programs to the mandated core program. DoD's training goal should be continuous information-security awareness, at all levels. This cannot be accomplished by the current annual one- or two-hour course.[15]

[14] Currently, OSD (C3I) is beginning this effort within the Pentagon. The sooner this program is implemented DoD-wide, the sooner the integrity and continued functionality of DoD's network and data base systems will better ensured.

[15] SSG IV was impressed with training programs at CITIGroup, Lockheed-Martin, and Caterpillar.

➢ People

Premise: *That people are the key to continued U.S. military superiority in the 21st century; therefore, increased emphasis must be placed on recruiting and retaining quality people.*

The United States will continue to maintain significant military capability in the 21st century to protect American interests, both at home and abroad. There are no apparent technological "silver bullets" enabling the U.S. to reduce military manpower requirements significantly, despite expectations by some that the information revolution may bring about reductions. The requirement to maintain large, educated, and motivated armed forces, despite growing military personnel shortfalls, shows that present concerns about recruiting and retention are clearly justified.

Premise: *That maintaining an all-volunteer force in a robust economy requires a military compensation package that is competitive with civilian industry.*

We demand much from our people, including acceptance of the risks inherently associated with military operations. We should pay our people accordingly. The 4.8% pay raise that is included in the FY2000 budget is a small step in the right direction (+$48 per month for an E-1; +$182 per month for a 0-4 with more than 10 years service). The targeted pay raises scheduled for July 2000 will provide additional pay relief. Nevertheless, the FY 2000 military pay raise would have a greater psychological impact if it were included in an emergency supplemental for immediate implementation this year, instead of taking effect on 1 January 2000. The next Quadrennial Review of Military Compensation is just getting started and will take about eighteen months—which is too long, given the urgency of solving military recruitment and retention problems. Therefore, a special committee should be formed, and it should be given six months to review the entire range of military compensation issues.

Premise: *That most people don't join the military for money; so just increasing pay will fail to solve the current recruiting shortfalls or stem the exodus of experienced personnel.*

The Navy periodically surveys new recruits to understand better their motivation for joining the Navy. Survey data indicates 49% of recruits join for college or skill training, 19% for travel, 10% for pay and benefits, and 4% to serve their country.[16] Recruits have different motivational factors than people already serving in the military, however, so the needs of these two groups must be analyzed separately. The top reasons junior officers give for leaving the Navy are: loss of job satisfaction; unnecessary work (weekend work preparing for inspections); micro-management; a zero-defect mentality; erosion of benefits; and lack of confidence in leadership.[17] The top reasons given by Air Force pilots

[16] "Navy New Recruit Survey", Navy Recruiting Command, May 1998.
[17] Rear Admiral John T. Natter et al., "Listen to the JOs: Why Retention is a Problem," U.S. Naval Institute *Proceedings*, October 1998.

for leaving the Air Force are: high operating tempo; quality of life (too much time away from home); airline hiring; and staff assignments being too long.[18] In recruiting, we should focus on educational opportunities and the adventure of military life. In retention efforts, we must address not only pay, but also quality-of-life and job-satisfaction issues.

Premise: *That military life involves significant personal sacrifices; national leaders need to explain clearly the rationale behind the deployment and employment of military forces to justify these sacrifices.*

The Cold War gave us a monolithic enemy as the focus our efforts. Most who joined the military before the fall of the Berlin Wall joined with the idea of defending the American way of life against Communism. Today the United States does not have a specific enemy. We recruit young men and women to be warriors, but how is that defined? Today's armed forces are more apt to be peacekeepers and providers than traditional warriors. This broad and not always well-defined role requires clarification and validation at the national level. Also, a coherent explanation of U.S. "national interests" involved in deploying troops to places like Somalia, Bosnia, and Kosovo must be articulated. If this is not done, then potential recruits, their parents, and active-duty personnel will question whether such operations are worth the risking of their lives, and without a clear statement and understanding of national interest, the answer might well be "no."

[18] LtCol Frasz, HQ AF/DPFFF, "The Air Force Pilot Retention Story," USAF Staff Working Paper, 25 Nov 98.

➢ Experimentation

Premise: *That rigorous experimentation, both joint and service, is needed to ensure that future war-fighting concepts are developed, tested, and integrated.*

Developing a culture of experimentation encourages innovation throughout the force, an essential element in maintaining U.S. military advantage. Successful experimentation requires the constant evaluation of technology and its effects on operational concepts, and on the impact of emerging operational concepts on the search for new technologies (see Figure 1). Experimentation includes the use of "red teams," which are used to challenge emerging and refined operational concepts to find asymmetric and symmetric vulnerabilities. There also should be a method for integrating both Joint and Service experimentation outcomes to ensure that they are complementary and result in better joint interoperability. In addition, DoD, Joint, and Service leadership must recognize that failure is part of experimentation, and that experimentation must be inculcated into DoD as a continuous process. Finally, closure on experimentation can be achieved only if there is an end-to-end system ensuring that experimentation results become doctrine and alter acquisition programs and processes accordingly.

Premise: *That DoD should invite allies to participate in the DoD experimentation process, to ensure interoperability with allies and gain insights into their thinking, consistent with overall U.S. foreign policy and National Security Strategy objectives.*

The current National Security Strategy (NSS) and National Military Strategy (NMS) emphasize the U.S. desire to participate in military operations with coalitions. To achieve this, allies must become truly interoperable with U.S. forces. Interoperability has been defined in the past as the ability to exchange information and have certain hardware compatibility; in the future, having compatible operational concepts will become critically important. In addition, allied participation could help expose symmetric and asymmetric vulnerabilities in our operational concepts, while providing us with insights into their operational concepts. Future allied interoperability and our ability to conduct combined operations will depend not only on hardware and software compatibility but also on shared understanding of operational concepts—which will result from integrating allies, potential allies, and coalition partners into U.S. experimentation processes.

Premise: *That experimentation organizations, whether service or joint, must be properly resourced, staffed, and funded.*

Experimentation must become part of our warfighting culture. Future military advantage requires a dedicated commitment to experimentation today, to ensure our advantage in the future. Failure of DoD and military leadership to resource and support experimentation properly could result in a Congressionally mandated or directed experimentation process. Support for experimentation must include integrating experimentation results into both the doctrine-development process and the acquisition system. Actions on the part of DoD, Joint Staff, and service leadership must reflect their

commitment to the experimentation process, particularly through the assignment of enough people, facilities, and resources to ensure success and prevent the loss of U.S. military advantage to a more daring opponent.

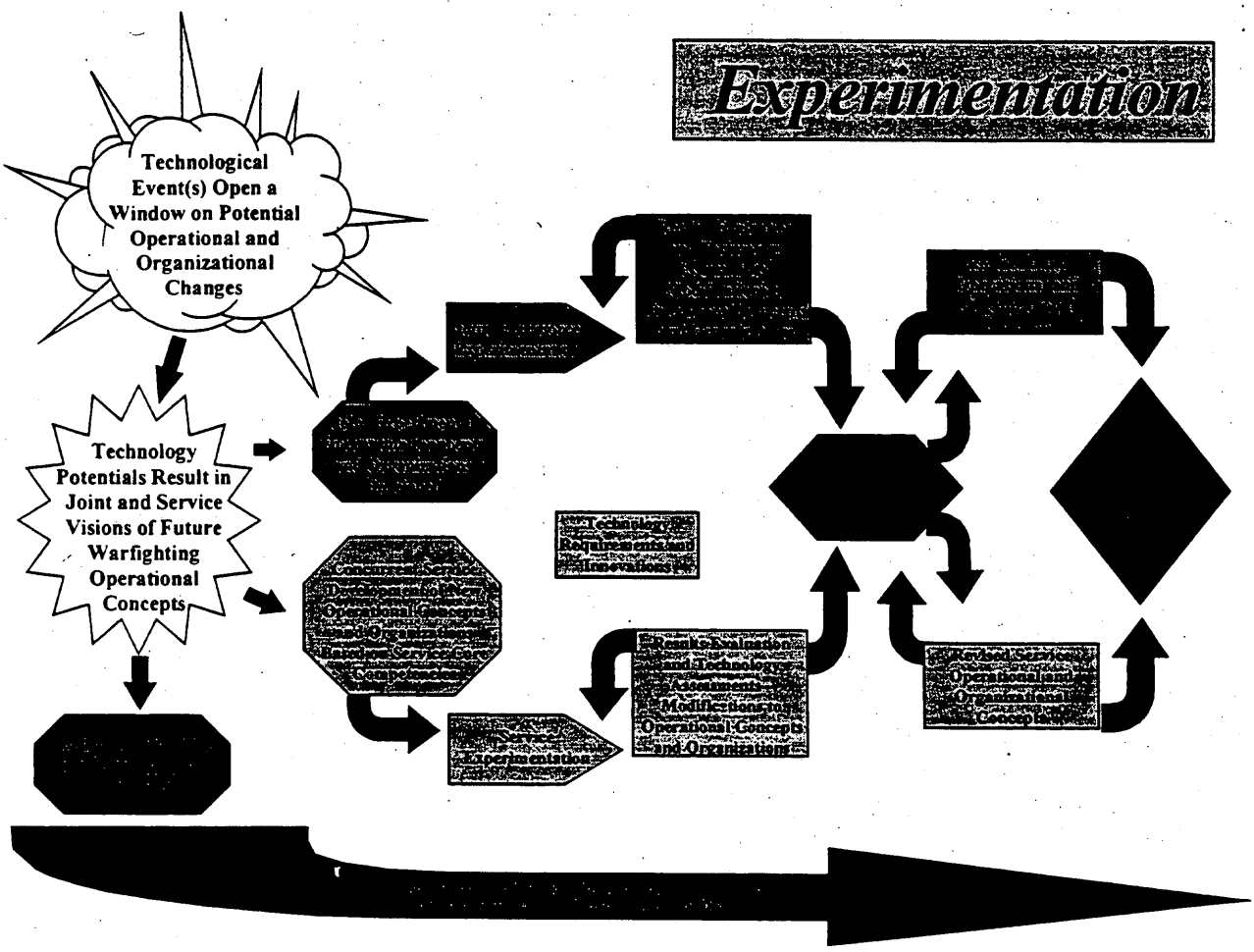

FIGURE 1

➢ Space

Premise: *That DoD must ensure U.S. access to the critical dimension of space.*

Space holds opportunity for both the United States and its adversaries. The international commercialization of space provides adversaries with otherwise unavailable capabilities, while offering the United States both a less costly avenue to space and potential business opportunities. Given the growing commercialization of space, DoD should outsource its space requirements when economically and militarily prudent, but retain an ability to reconstitute access to space if commercial access should be challenged. This ability to reconstitute is dependent in part on protecting some technologies: e.g., space launch. Other technologies, however, should be offered on the open market—creating both commercial opportunities for U.S. companies and international dependency on U.S. technology.

Premise: *That the ability to deny access to space must be developed.*

The commercialization of space has created a global interdependency on common space assets. As a result, this reliance on common assets could neutralize space in time of conflict—with allies and adversaries both reluctant to attack space assets for fear of diminishing their own capabilities. DoD must invest in the means to neutralize space assets—both commercial and military—while retaining the ability to reconstitute as needed. In order to neutralize—and selectively deny access to—space, DoD must develop the means to control and destroy space assets (both in space and at ground level), while selectively reconstituting its own capabilities through multiple sources.

➢ National Level Premises

Premise: *That DoD needs to request coordinated national responses to security issues rather than military solutions alone.*

The U.S. is likely to face future conflicts that lack the traditional military characteristics of the past. Furthermore, the strained U.S. defense budget and the increased operations tempo trend in recent years will limit DoD's ability to be everywhere and do everything. Traditional military forces will remain critical to national security over the near term, but increasing the overall effectiveness of U.S. responses will depend more on how well the United States can coordinate the actions of all the various government agencies and non-governmental organizations. More effective application of U.S. power will require a level of interagency coordination much higher than presently exists. DoD should work within the executive branch to devise a more responsive organizational structure and procedures to develop, coordinate, and implement national crisis-response strategies.[19]

Premise: *That DoD, in conjunction with the national leadership, needs to develop a better way of explaining "Why Defense?" to the American people.*

A number of factors are making it increasingly difficult to justify resource expenditures for defense, and to recruit enough volunteers to serve in the armed forces. The declining number of World War II veterans and absence of a draft since 1973 continue to erode the powerful informal "network" that used to spread the word about the U.S. military. Most of the American public has no military experience or contact with active-duty military personnel. A significant segment of the public has no interest in foreign affairs and lacks understanding of the military's role in supporting U.S. policy objectives around the world. There are other indications of inadequate understanding of the role of the U.S. military: recruiting is becoming increasingly difficult; and people within the military are leaving, owing to their confusion about the current role of the armed forces. DoD should aggressively develop and implement an effective, long-term public relations effort, which tells the story of "Why Defense?" to the American public.[20]

---

[19] The rapidity of action envisioned in the Information Age demands more agile, responsive organizations and processes than exist in the current government bureaucracy. One high-level official the SSG interviewed described Presidential Decision Directive-63, subject: Protection of the Nation's Critical Infrastructure, as "all nouns, no verbs" to explain why the document lacked the necessary guidance to make the government responsive to an attack on critical infrastructure. Also, it is worth noting that another official told the SSG that "crisis response" exercises—meant to train senior decision-makers and find shortfalls in organization and processes—were typically attended by second, third and even fourth-tier decision-makers. The inference is that when the first-tier decision-makers are faced with a real world crisis in the Information Age, the shortfalls in the Cold War organization and processes will become obvious, but it will be too late.

[20] The Secretary of Defense's recent initiative to tell the story of "Why Defense?" is a significant step in the right direction. A similar effort by other senior leaders in government, especially the President, would be an immeasurable contribution to improving public awareness about the importance of the U.S. military.

Premise: *That DoD needs to clarify its role in responding to domestic/internal security threats.*

Information warfare, the increasing availability of weapons of mass destruction or disruption, and other asymmetric tactics an adversary may attempt to employ against the U.S. have brought renewed emphasis on the concept of "homeland defense." There is some confusion about how to respond to an attack on critical infrastructure when it cannot be determined quickly who is attacking and what they are trying to accomplish. At present, DoD has the lead only for external security (i.e., applying force outside the geographic borders of the United States). Fourth Amendment restrictions, computer privacy laws, and other laws such as *Posse Comitatus*[21], do not allow unfettered, rapid response to information attacks (e.g., it is illegal to "hack back"). DoD's role in homeland defense is therefore circumscribed, which could inhibit projection of military power abroad.[22] DoD should insist on the resolution of this issue to ensure that it can respond—in conjunction with other executive departments and law enforcement—in the most timely and effective way to defend our homeland.

[21] 18 U.S.C. 1385. It is by national policy, not statute, that the Navy and Marine Corps are included in this restriction.

[22] For example, if an adversary successfully disrupts the infrastructure that DoD relies upon to support its power projection capability, it could have a negative effect on rapid deployment into a theater of operations. It is imperative that the U.S. be able to counter rapidly any attack on critical infrastructure.

Annex A: PROTECTING MILITARY CAPABILITY

A METHODOLOGY

1. **Observation:** *Joint Vision 2010* provides a vision for transformation of the military to stay ahead of future security challenges, but there is no adequate process in place to get there. Today, the Department of Defense is unable to provide the Secretary of Defense with an integrated perspective on the criticality of military capabilities and their importance to future warfare. Nor is there a systematic process for determining actions the United States must take to sustain global military dominance into the next century. The absence of an authoritative "short list" of critical capabilities denies the Secretary of Defense the tool he needs to present Congress a coherent funding plan, which meets future national security imperatives while sustaining near-term force readiness.

2. **Purpose:** This paper proposes the institutionalization of a process through which the DoD can identify rationally the existing and emerging technologies and operational concepts that have the greatest potential to help sustain global military dominance in an uncertain future.

3. **Background**

a) There are a number of strategies, plans, and objectives produced by DoD in response to the Secretary of Defense's vision to "develop and transition superior technology to enable affordable, decisive military capability." They include:

1) ***Defense Science and Technology Strategy***. An overall S&T strategy to address the Joint warfighters' stated needs, maintain a broad-based program spanning all defense-related sciences and technologies to anticipate future needs, support the unique needs of the military departments, preserve long-range research, and do it all within limited budgets.

2) ***Basic Research Plan***. Includes DoD objectives and investment strategy for DoD-sponsored basic research (6.1) performed by universities, industry, and Service laboratories. The plan also highlights the research objectives that have the greatest promise for the development of breakthrough technologies with military applications for the 21st century.

3) ***Defense Technology Area Plan***. Presents the DoD objectives and applied research (6.2) and advanced technology development (6.3) investment strategy for technologies critical to DoD acquisition plans, service warfighter capabilities, and the Joint Warfighting Science and Technology Plan (JWSTP). It provides a horizontal perspective across the Service and Defense agency efforts.

4) ***Joint Warfighting Science and Technology Plan (JWSTP)***. This plan takes a joint perspective horizontally across the applied research (6.2) and advanced

technology development (6.3) plans of the Services and Defense agencies to ensure S&T program support priority for future warfighting capabilities.

5) ***Defense Technology Objectives (DTO)***. Identifies specific technology advancement that will be developed or demonstrated, the anticipated date of technology availability, the specific benefits resulting from the technology advance, and the funding required to achieve the new capability.

b) The principal tool employed today to identify critical technologies is the ***Militarily Critical Technologies List*** (MCTL), a detailed and structured compendium of the technologies DoD assesses as critical to maintaining superior U.S. military capability. It is a documented snapshot of the continuous MCTL process. The MCTL, with its legal basis in the Export Administration Act of 1979, principally is a vehicle for evaluating potential technology transfers and technical reports and scientific papers for public release. The list is developed by Technology Working Groups (TWG), composed of technical experts from the armed services, DoD, and other federal agencies, industry, and academia.

c) In the near future, the MCTL will be published in three parts: Weapon Systems Technologies; Weapons of Mass Destruction; and Critical Developing Technologies. Absent from the process and products are existing and emerging foreign technologies.

d) In essence, the MCTL is a product of the Science & Technology community. In its present form it has little utility beyond evaluating potential technology transfer. Its size alone begs the question of whether it is a military-critical list or an all-inclusive list. Nevertheless, the MCTL is the most comprehensive process of its kind in the defense community. It is written in a common language that many in government and industry understand and feed with appropriate data.

4. **What's broke?**

a) Sustaining U.S. military superiority will require a careful balance between maintaining relevant legacy forces, facilities, and systems and developing new capabilities. DoD's current S&T vision, strategy, plans, and objectives focus on four areas: affordability; dual use potential; accelerated transition; and a strong technology base. It is imperative that DoD shift its emphasis from a strategy that lost its relevance at the end of the Cold War, to one that capitalizes on the advantages and avoids the risk inherent in accelerating globalization of industry and the ongoing transformation of business practices in the Information Age.

b) In the absence of an effective methodology to define clearly a short list of key military capabilities that should be developed and protected, the tendency has been to overprotect. This safesided approach limits the ability of U.S. industry to pursue market leadership in selective military and dual-use technologies. DoD strategies must evolve to account for the technology leveling that will occur as a result of globalization, and apply greater attention to the importance of U.S. economic vitality and diversity in the global

marketplace. The combined impact of globalization and commercialization suggests the need for a new partnership between government and industry. Our collective strategies should orient our efforts toward leveraging the impact of globalization, commercialization, and Information-Age technology to sustain global military dominance.

5. **The Fix:** An institutionalized body of the right players, who meet on a recurring basis (supported by a structured process) to match our most important operational concept (warfighter task) with the art of the possible (S&T task)—and subject the results to experimentation—could serve to:

a) Identify a short list of militarily critical capabilities, technologies, and operational concepts that must be protected from diffusion and subjected to extraordinary export control, and sustain or enhance US military superiority. It should be noted that criticality may reside within a technology, a system, a component, a process, a design, production, utilization capability, or plans, policies, and concepts. To remain relevant, the list must be a living document, which can be updated with a frequency that recognizes ever-decreasing cycle times.

b) By design, the process of distilling a larger menu of military capabilities into an authoritative short list of critical capabilities offers a number of significant benefits. In addition to providing the Secretary of Defense with a tool to help define DoD acquisition priorities, it could:

1) Support the development of specific strategies with the balanced objectives of staying ahead with critical capabilities, while protecting the same capabilities from premature compromise.

2) Serve to label the technologies that should not be subjected to U.S. protection. The product would be DoD input to U.S. export control policy.

3) Help accelerate our military transformation by further integrating emerging technologies with evolving operational concepts.

4) Focus technology and capability sharing in a way that cultivates U.S. relations with future global power centers.

5) Cultivate dependencies and embrace leading foreign technologies in support of DoD and U.S. foreign policy objectives.

6) Identify those technologies that fall below the short list and above the no controls list for continued application of existing export control.

7) Further promote U.S. global market leadership.

6. **Concept:** A proposed methodology for determining future critical military capabilities is outlined below and depicted graphically in Figure 2.

a) The key to success is the composition of the working/steering groups. Current technology lists are developed and managed by the best efforts of the S&T community. What has been missing is a short list of key military capabilities. The imperative must be to bring together the warfighter and the S&T community in a way that enables DoD to rationalize and prioritize the warfighter's desired military capability with the S&T community's art of the possible, without chasing technology.

b) The working/steering groups must be supported with three products. First is an authoritative strategic template, reflecting our collective best view of future threats and challenges DoD must be able to address. Second is a comprehensive understanding of the required capabilities, and the few key areas of warfare the CinCs and military services seek to sustain or develop in the future. Finally, there is a list of significant U.S. and foreign technologies (existing and emerging) that must be developed to support the front end of the process. Conceptually, the MCTL could be adapted to meet this requirement. In addition, it should be screened to identify the technologies that will be difficult to protect or already are available in the global marketplace.

c) The sequence of activities and products developed by the process would look roughly like this:

1) The initial charter of the working group would be to take the front-end products mentioned above, explore the art of the possible, and identify critical capabilities and technologies as they apply to three general areas: Sustaining U.S. military superiority; empowering a U.S. emulator; or enhancing the capability of a state or non-state actor to attack the United States asymmetrically. While addressing asymmetries that could be exploited by others, the effort must also single out those powerful asymmetrical capabilities possessed by U.S. military forces that should be subjected to protection. The product would be a first cut at three short lists.

2) The short lists then would be circulated within the participating departments and agencies, to leverage the collective wisdom. Upon consolidation of input, a steering group would meet to review the results and prioritize candidates for field/fleet/aerospace validation and recommend proponency. Vehicles used for validation would include Service, Joint, and combined experimentation, exercise programs, battle labs, and Advanced Concept Technology Demonstrations (ACTD).

3) Specific objectives will be developed to explore selected warfighting capabilities and technologies through experimentation. Validation could occur as a result of Joint, combined or service experimentation. ACTDs and Service Battle Labs also may be employed to help explore the objectives.

4) Upon completion of the validation phase the working/steering group will review the results, prioritize (rank order) the technologies, and propose DoD input to export control policy.

5) The final product is a living document that captures those technologies and military capabilities that best represent the sources of global military advantage in the future. Upon review and approval by the DoD leadership, the short list may be used to support resource allocation decisions. As an example, a significant capability or technology identified that has great potential to sustain or enhance U.S. military superiority could be identified as a candidate for a "spend hard, run fast" strategy to attain "first-mover advantage."

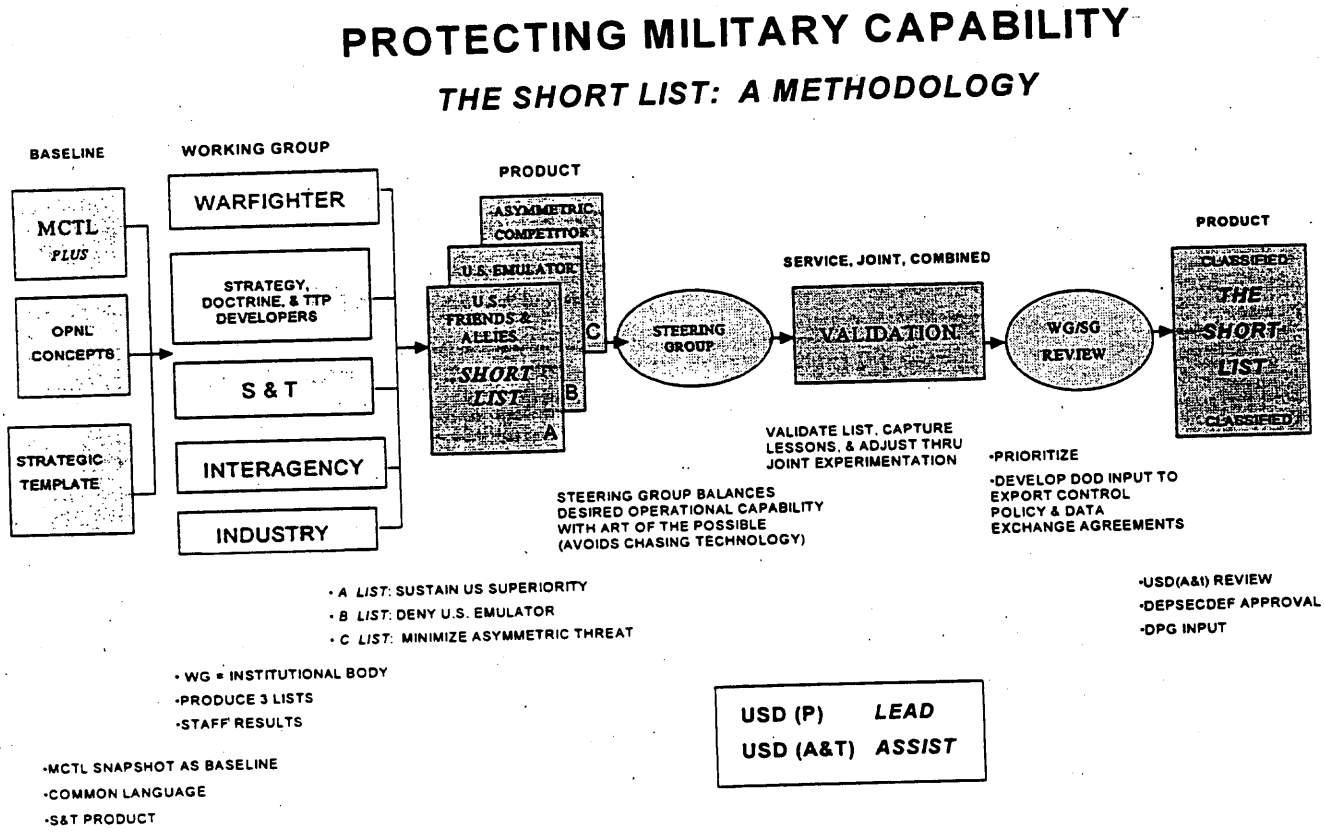

FIGURE 2

7. Conclusion

a) The globalization phenomenon is altering the requirements for sustaining military dominance in the 21st century. In light of this changing environment, we must shift our priorities toward exploiting advanced commercial technologies from the global marketplace. In addition, we must leverage DoD leadership in military-unique technologies that will help sustain U.S. military superiority.

b) This study concludes that it is possible to develop a mechanism to determine criticality in our military capabilities and operational concepts. To move ahead, DoD must:

1) Bring the warfighter community together with the S&T community.
2) Develop an extensive and systematic process that evaluates future objectives, threats, vulnerabilities, strategies, technologies, and generic capabilities.
3) Produce a validated short list of key military capabilities.

c) The results of such a process are manifold. They would:

1) Help define DoD acquisition priorities.
2) Refine DoD's position on the control of military technology to sustain military superiority.
3) Align contractual and regulatory structures between DoD and defense industry.
4) Provide the Secretary of Defense with a powerful vehicle to help articulate defense requirements to Congress.

d) Ultimately, DoD must move away from purely military responses to crises and enlist the support of the interagency, industry, and academia to address national-level responses to future crises. In the interim, institutionalizing a process like the one outlined in this study could produce an important tool in pursuit of *Joint Vision 2010* by providing much needed focus for the transformation to a 21st century force. The intent must be to harness and drive commercialization and globalization, rather than be driven.