Policy and Social Barriers to New Military Information Technologies

Paul J. Feltovich, Jeffrey M. Bradshaw, Larry Bunch, and Matthew Johnson

Florida Institute for Human and Machine Cognition (IHMC)
Pensacola, Florida
{pfeltovich, jbradshaw, lbunch, mjohnson}@ihmc.us

26 March 2010

Contents

1 Introduction

Many studies have documented the daunting nature of modern, network-centric military operations. Such operations implicate diverse and often ideologically driven stakeholders; fluidly configured, opaque, well-informed, and adaptive adversaries; highly (even globally) distributed operations and operational fields; and increasingly sophisticated technologies used either to support or undermine these kinds of complex enterprises. Frequently, conflicting, outdated, or cumbersome objectives, policies, and procedures impede the effectiveness and timeliness of new military technologies (Charette, 2008; Gates, 2009). This is especially true in operations involving multi-agency, security-sensitive, or highly time-bound operations (e.g., Davis et al., 2007). Though the needs for timely technology development and deployment have become more acute, many of the basic challenges are not new, tracing back to the beginnings of US military acquisitions (MacNaugher, 1989).

In this report, we identify and characterize several classes of policy and social barriers to the creation and deployment of new military information technologies. Though not exhaustive, our inquiry is broad, including not only pertinent “black-letter” policy (e.g., DOD directives or executive orders), but also impediments that are caused or exacerbated by organizational structures and lines of authority, engrained roles and practices, and other historical, cultural barriers—across and within the many and diverse groups involved in modern military, and related intelligence, operations (DOD Directive, Petraeus, 2006; Zinni & Koltz, 2006). In the current version of this report, we do not consider *technical* barriers per se, what we have elsewhere called “little p” policy in contrast to “Big P” policy (Bradshaw *et al.,* 2003, 2004).

We consider this report to be a living document that will be updated as new information becomes available. However, it is important to make clear that the report is only one among several avenues of inquiry that are being pursued as part of this research program. For example, a survey of pertinent science and technology professionals will be undertaken to help elaborate hypotheses generated in the current report and to probe further into questions and concerns the report leaves unanswered or unaddressed.

In the next section, we summarize the R&D objectives defined in *Joint Vision 2010*, and give a brief example of how military acquisitions can go wrong due to policy issues. We then identify and characterize several types of policy and social barriers that can stand in the way of innovation and timely deployment of new ideas and technologies on the battlefield. Five in particular are discussed: 1) the materials acquisition process itself, 2) the need for increased user participation in design and development, 3) challenges of interagency relations, 4) conflicting requirements for legality, security, and effectiveness, and 5) problems posed by closed systems and hyper-caution. Within each of these topics, we address both the challenges posed and also current thinking about how the problems can be alleviated and what further questions need to be asked.

2 The Nature of the Challenges

Modern US military operations face challenges for which there is limited precedent, but even worse, ones that can change quickly. We outline some major objectives of DOD, and then give an example of how policy gone awry can negatively affect warfighter safety.

2.1 Major DOD Research and Development Thrusts

Some years ago, the Department of Defense (DOD) defined five priority thrusts for research and development. These objectives were defined and adopted as part of Joint Vision 2010, under the direction of the Defense Science & Technology Program (S&T), as validated by the Joint Requirements Oversight Council (Etter, 2001, pp. 168-172). The objectives were:

1) *Information assurance*. Protection and assured use of large-scale information networks.
2) *Battlespace awareness*. Tools to enhance useful situational awareness in chaotic environments.
3) *Force protection*. Protection of the fighting force itself, across highly diverse and often unanticipated operational environments.
4) *Reduced cost of ownership*. Reduction of cost across the whole spectrum of acquisition and employment.
5) *Maintaining basic research*. Maintaining a healthy basic research program amid ever-increasing pressure for quick turnaround of science and technology products.

These general themes are entwined within the body of the report, as they relate to our topic. For example, the next section provides a vivid story of force protection, or, more accurately, the lack of it.

2.2 Public Example of Policy Negatively Impacting Warfighter Safety

In 2008, American soldiers on missions in Iraq and Afghanistan were being killed by Improvised Explosive Devices (IEDs). Many of these devices took the form of roadside bombs that exploded as vehicles passed by. Most of the vehicles available to the troops were not adequately armored to withstand such blasts, as had been the case since the inception of the operation in 2003. Also in 2008, it was revealed that many more-substantial vehicles could have been deployed long before, but had not been. This was seen by many as scandalous and, as often happens in such instances, the U.S. Congress intervened to explore the revelations. Two senators called for action:

> ***Senators Seek Investigation of MRAP Delay***
>
> Senator Biden (D-DE) and Senator Bond (R-MO) are reportedly seeking answers to issues raised in a report written by a civilian official for the United States Marine Corps. The report alleges that a request for mine-

> resistant, ambush-protected (MRAP) vehicles was denied sometime around 2005 due (in part) to cost-related concerns.
>
> Senator Biden was quoted as saying: “This is a stark warning that the military brass back home is not acting on needs of our warfighters on the front lines. We must be as fast and flexible as the enemy. We need an official investigation to figure out why this happened and to make sure it never happens again.”
>
> Senator Bond stated: “With our troops serving on the front lines in the war on terror, this gross mismanagement of our military’s acquisition process is inexcusable. The military needs to take a hard look [at] the bureaucratic delays of lifesaving equipment to our troops in the field.” (*Senatus*, 2008)

Phrases like “Why did this happen?” “We need to make sure it never happens again,” and “bureaucratic delays,” often invoke matters of policy—either as forms of prevention and remediation, (e.g., “Why weren’t there policies in place to prevent this?”), or as barriers to progress (e.g., “We can’t function with all this red tape!’’). Indeed, the adoption of new, and enforcement of existing, policy seems to be heightened after episodes of crisis (Gerding, 2006).

Policy issues regarding the armoring of vehicles in Iraq predate the inception of MRAP by many years, harking back to a time when there was no armoring, IEDs were killing soldiers daily, and US soldiers took to “armoring” their own vehicles by welding on scrap metal they found in Iraqi dumps. With regard to their safety, the soldiers were conducting their own, on-the-spot, military equipment acquisitions program—including on-the-spot research and development. This was long before the official military procurement process regarding this matter, including its structured stages of research, development, and testing, kicked into play (DSB06, pp. 6-8). That process is still grinding on—as evidenced by the ongoing MRAP controversy just discussed. Another striking example has also gained considerable recent attention: the F-22 fighter aircraft was ten years late going into production, 226 million dollars over budget, and has yet to see significant action in combat (Charette, 2008).

3 Important Categories of Barriers

3.1 Acquisition-Related Barriers

Many factors influence the speed, timeliness, and effectiveness of technology development as it proceeds from conception to actual use within military operations. We take up some of these factors in this section.

3.1.1 The problematic nature of the acquisition process

The lengthy process of proposal preparation and awarding, research, development, and testing—influenced and often delayed at every step by policy—can greatly degrade the timeliness and effectiveness of new technologies. These concerns, of course, affect the development of new hardware, but perhaps have an even greater impact on software and information technologies due to the fact that they are subjected to additional scrutiny, as we will discuss below. The acquisition problem has been well studied over the years. For instance, the 1986 Packard Commission concluded that the slow and unresponsive acquisition process leads to: "unnecessarily high cost of development, to obsolete technology in our fielded equipment, and it aggravates the very gold plating that is one of its causes" (DSB06, 2006, p. 1; see also, McNaugher, 1989).

Despite repeated calls for reform, a 2008 report makes it clear that serious impediments still remain:

> This desire for shorter acquisition cycles is not new… For example, a 1994 Congressional report asked for "a 50 percent reduction in cycle time;" a 1996 White House report requested a "25 percent cycle time reduction for major defense acquisition programs by 2000" (from a then-historic average of 11 years); a 1997 high-level DOD council stated they wanted to "aim for a 50 percent reduction in acquisition cycle time" (implemented in DOD policy directives); the 2001 Quadrennial Defense Review and the 2004 National Military Strategy requested "rapid adjustment to changes in the environment;" and numerous prior Defense Science Board reports … have all strongly urged "greatly reduced acquisition cycles." But the empirical data … show that as the complexity of weapons has greatly increased, and the focus of the acquisition system has continued to push the state-of-the-art to its extreme—emphasizing maximum performance at the expense of delivery time and cost—*the actual schedules for most weapon systems have been increasing.* (DSB06, 2006, abstract, emphasis ours; see also Charette, 2008; Gates 2009)

Acquisition procedures and complexities were not as much of a problem during what are now viewed as "traditional" wars, including the Cold War, when the speed of developments and adaptations among the adversaries occurred over longer time spans. Unfortunately, a recent report found that:

> Acquisition policies, practices, and processes are still Cold War-based. Technology development and fielding is governed by measured, sequential events that are paced by the PPBE[1] process that requires extensive coordination and concurrence by multiple functional communities (logistics, security, personnel, etc.). (DSB06, p. 78)

Overcoming the bottlenecks of the acquisition process has become increasingly urgent as we simultaneously confront multiple instances of new kinds of war across the planet—with unanticipated breakouts, rapid development, new kinds of actors, adaptive adversaries, and sometimes highly unconventional methods (cf. DSB06, p. iii).

[1] Defense Planning, Programming, Budgeting, and Execution

Within the Army, the long trail of the acquisition process often starts with the DARPA and the Army Research Laboratory (ARL), which generally manage basic (6.1) research. Research and development ideas must then flow through processes of "basic development" (6.2), "exploratory development," (6.3, 6.3a), "prototyping" in the field (6.3, 6.4), following by a program-manager-directed deployment of the new asset. In contrast to this largely sequential "waterfall" process, best practices in the private sector have followed a "spiral" development process for decades. Consistent with a human-centered design approach and following a cognitive task analysis methodology (e.g., Flanagan, *et al.*, 1997; Hoffman, *et al*., 2000), the spiral methodology recommends that rapid prototypes be developed with participatory design by end users from the earliest phases of the project and that these prototypes be matured through constant iterative refinement. In this manner, downstream "surprises" in the context of deployment can be minimized. This approach is discussed in more later in the report.

The length of the acquisition process increases costs and the likelihood of technology obsolescence—or even irrelevance to the intended users. One ARL Program Manager (PM) consulted for this project made the comment that by the time a technology passes through all of these stages and is ready to be manufactured and fielded, some of its components may be obsolete or unavailable in normal markets, forcing acquisition through secondary, specialty markets at higher price. A specific instance of components becoming obsolete or unavailable, and having to be changed even *during* the long development process itself, is given by Charette (2008, p. 36).

DOD research organizations typically work in partnership with state and local governments and private sector organizations that assist in research, development, and marketing of products ("technology transfer."). Policy and organizational culture barriers also pervade this process:

> Congress has established a system to facilitate the transfer of technology to the private sector and to state and local governments. Despite this, use of federal R&D results has remained restrained, although there has been a significant increase in private sector interest and activities over the past several years. *Critics argue that working with the agencies and laboratories continues to be difficult and time-consuming.* (Schacht, 2007, summary, p.i, emphasis ours)
>
> …ambiguities associated with obtaining title to or exclusive license for federally owned patents also contribute to a limited level of commercialization. Complicating the issue is the fact that the transfer of technology is a complex process that involves many stages and variables. *Often the participants do not know or understand each other's work environment, procedures, terminology, rewards, and constraints.* (Schacht, 2007, p. 3, emphasis ours)

3.1.2 Lengthy additional screening for networking and information technology

In addition to the usual requirements for development and implementation, networking and information technologies must undergo an additional process of screening. This involves the TEMPEST certification process, conducted by the National Security Agency (NSA—http://www.nsa.gov/ia/industry/tempest.cfm). This process examines new technologies in order to detect vulnerabilities to encroachment or leakage of information vital to national security. This added layer of certification compounds an already long acquisition process for these kinds of vital technologies.

3.1.3 The need for changes in technology to address new kinds of conflict

Despite considerable lip-service, research and development for the new kinds of defense and military operations (e.g., SSTR operations, Stability, Security, Transition, & Reconstruction; DOD Directive, 2005) is not being adequately promoted, enacted, and rewarded. The new modes of operation are foreign to long-standing military culture, outside traditional skills and practices, and are not, at least at present, considered fertile tracks for rewards and promotion (Gates, 2009).

Another major change in recent years is that the kinds of equipment and arms needed are sometimes quite different from those that have been useful in more traditional combat. These new technologies may sometimes even be easier to create and deploy, relying on high quantity and lower tech capabilities—e.g., thousands of simple sensor devices or networking tools, versus a small number of hugely sophisticated aircraft requiring a decade or more of development (Charette, 2008; Gates, 2009).

3.1.4 Decreased emphasis on basic research

As we have noted, the nature of the new military operations is causing great pressure to decrease the length of the acquisition cycle. In this growing trend, 18 months is now considered a "long-term" horizon, 6-12 months "intermediate," and 3 months "short term." While the desire for timeliness and adaptive capability is understandable, the methods have not always been sound. For example, many of the speed-ups involve unproven shortcuts to existing methods rather than rethinking the basic paradigm (e.g., waterfall vs. spiral development). A big loser in this accelerated process has frequently been basic (6.1) research, seriously compromising the possibility of future breakthroughs that are vital to a rapidly changing battlefield. In the past, such research has provided invaluable breakthroughs such as Kevlar, stealthing, and lasers, to name a few.

> An investment in basic research pays dividends in many ways. Basic research is a long-term investment with emphasis on opportunities for military application far in the future. It also contributes to our national academic and scientific knowledge base by providing approximately 40 percent of the support for all engineering work. The Department sustains its investment in basic research because of proven, significant, long-term benefits to the military, which in turn enhances our national economic security.
>
> Basic research provided the foundation for technological superiority in each of

> our recent conflicts. Radar made a significant contribution to winning World War II. Stealth, lasers, infrared night vision, and electronics for precision strike played major roles in the Gulf War. Adaptive optics, phased array radar, and global positioning systems (GPS) also contribute to our readiness. Our nation's defense advantage is founded on a wide scope of scientific and engineering knowledge. The Department must continue to invest broadly in defense-relevant scientific fields because it is not possible to predict precisely in which areas the next breakthroughs will occur. (Etter, 2001, p. 171)

Concerns about the health of basic science may, at first, seem in conflict with the need for tighter and faster coupling of research and the battlefield. The great dilemma is that, indeed, we need to find ways to accomplish both.

3.1.5 Current efforts to address acquisition-related barriers

Responding to the problems associated with the cumbersome acquisition process may require a new approach to risk management:

> Technology development and fielding is (now) governed by measured, sequential events that are paced by the PPBE process that requires extensive coordination and concurrence by multiple functional communities (logistics, security, personnel, etc.). *The policies and rules have been set in place to ensure, to the extent possible, "no fault" acquisition and deployment of weapon systems and technology*. The need to be good stewards of the taxpayers' dollars and the national treasury is very important, but too often this mentality extends technology fielding times to points of obsolescence before fielding and fails to support the real needs of the warfighters. The intentions and spirit of current ways of transitioning technology have become dysfunctional to meet the current need. In the global war on terror, this can mean lives lost and opportunities squandered while the process operates. (DSB06, p. 78, emphasis, insert ours).

This statement raises a specific policy-related issue: the trade-offs in speed versus assurance (e.g., of quality, effectiveness, reliability) in the development and employment process. It is noted that perhaps, in the new war environment, "bullet-proofing" acquisitions (which invokes the role of lawyers) must give way to a greater degree to timeliness, along with its possible associated higher level of risk. Happily, as observed previously, adopting a human-centered approach to research and development may actually mitigate some kinds of risk (e.g., those associated with not involving the ultimate operator extensively enough) as it speeds deployment—thus offsetting in part such concerns.

Another attempt to address acquisition concerns has been the development of new transition mechanisms, positioned between the battlefield and the traditional acquisition cycle, and purposely designed to accelerate the pace of development while ensuring quality. For example:

> To speed up the technology transition process, three important mechanisms, Advanced Concept Technology Demonstrations (ACTDs), Advanced Technology Demonstrations (ATDs), and Joint Experiments, have been established to ensure the transition of innovative concepts and superior technology to the warfighter and acquisition customer both faster and less expensively. ACTDs are a key element in the S&T program. They are needed to determine the military utility of proven technologies, to expedite technology transition, to provide a sound basis for acquisition decisions, and to develop the concept of operations that will optimize effectiveness. They cover all technologies and provide rapid capability to the warfighter. (Etter, 2001, p. 174).

Another important recent example is the Urgent Universal Need Statement program—UUNS; MARADMIN, 2006). The success of these new mechanisms is under continual review (e.g., GAO05). However, it seems unlikely that these measures alone will solve the problem.

Other measures are being developed to address the sheer complexity, uncertainty, novelty, and current immaturity of basic technologies that the planning processes for future technologies must face. The emphasis is on the use of "business case" models to predict future military requirements and relevant technology gaps. The progress in this regard has been mixed. This has been reflected in the fits and starts associated with long development of the Future Combat Systems (FCS) initiative, which was initiated in 2003 and faces a significant progress review in 2009. In 2007, the GAO gave the following perspective:

> We look at a business case as comprising those elements that are key to making an acquisition likely to result in a product that performs as required for the time and money promised. A sound business case includes firm requirements; mature technologies; an acquisition strategy that demonstrates design and production maturity; and adequate funding to cover a realistic cost estimate. When FCS was approved to begin in May 2003, it was far from having a sound business case, especially given its unprecedented size and complexity. Specifically, requirements were not well-defined; technologies were very immature; the acquisition strategy was aggressive and did not allow for demonstrating design and production maturity until after the production decision; and despite the insufficient basis for good cost estimates, providing the resources at the estimated costs was a great challenge.
>
> Since then, there have been a number of improvements in the program. The schedule was doubled to allow for more demonstrations and to spin capabilities out to the current forces; requirements are better understood, even to the system level; technologies have gotten more mature; cost estimates have grown substantially, making them more realistic. Still, it is four years later, and progress should be expected. The Army, doing well by its own measures, is well behind business case measures. Requirements are still being

> defined; technologies are years away from needed maturity levels; key demonstrations of design and production will still come after the production decision; and independent cost estimates are significantly higher than the Army's. (GAO07, 2007, pp. 1-2)

3.2 Barriers to Human-Centered Design and Development

3.2.1 Designer-centeredness and human-centeredness

Within the military R&D program, the military labs (e.g., ARL, AFRL, ONR) are, along with DARPA, typically at the top of the acquisition chain. Within the long acquisition cycle, there is a concern that there is too much disconnect between some work of the DOD and military labs and the needs of warfighters. This is partly a matter of "human-centeredness" versus "designer-centeredness," in the R&D process (Hoffman, 2008, p. 72; Neville *et al*., 2008). The major difference in the two is that in human-centered processes, needs, development, testing, deployment, and incremental improvement all occur closer to the ground where the warfighter operates. This places emphasis on the needs of the warfighter, as the party closest to the application venue and the one with greatest personal investment in the quality and appropriateness of any new products or ideas:

> Any defense must begin with the warfighter, whose effectiveness is dramatically increased by advanced technology. Our nation relies on the technological superiority of our Armed Forces to maintain our position of world leadership. First and foremost, the mission of the Department of Defense Science and Technology program is to ensure that the warfighters today and tomorrow have superior and affordable technology to support their missions, and to provide them with revolutionary war-winning capabilities. To develop a strategy to support that mission we must understand the warfighter's needs and the full range of operations that must be performed by our military (Etter, 2001, p. 167).

There are many potential benefits to conducting R&D closer to the arena of use. These benefits include quicker access by the warfighter to the new tools themselves, as well as the provision for direct testing of their effectiveness and associated feedback to the design process:

> There is a tremendous incentive to the operational user to have all of these deficiencies [acquisition problems] eliminated. The user will get operational capability sooner and more relevant to the operational conditions. The user will be able to provide feedback to change needs in future spirals more quickly, based upon operational experience (DSB06, p. 81, insert ours).

This call for greater in-place participation and insight is not confined just to the warfighter, but extends to other operations and agencies close to the battle:

> Regardless of implementation decisions, military priorities developed without factoring in regional expertise from other U.S. agencies precludes the efficient and effective implementation of a vision. Until there is synchronization between engagement initiatives and foreign assistance, America loses opportunities to capitalize on comparative advantages, does not make the best use of resources, and could fail to reach strategic objectives. (Kelleher 2002, p. 4)

3.2.2 Current efforts to address barriers to human-centered design

One reaction to the perceived need for greater user-centeredness has been a call for greater employment of what is frequently called a "spiral" R&D process (DSB01, p. 23, insert ours):

> Spiral development is an iterative process that links users to developers through an approach that is common in commercial practice for continuous development and deployment of both hardware and software. The concept is to explore many technology options via experiments and ACTDs (discussed above). Those that demonstrate promise are rapidly deployed to the field in limited quantities as "Block 1" systems. Inherent in the process is that systems are likely to contain some weaknesses in Block 1 deployment, but increasing capabilities will be fielded in the subsequent blocks through a continuous development process. (p.23).

The general idea is that when a need is perceived on the battlefield, many quick-response options are actually put into play quickly, and they are further assessed, analyzed, and modified/upgraded in place in conjunction with the research of DOD and public sector labs that are not likely to be co-present.

3.3 Barriers to Inter-organizational Synergy

Yet other impediments to the development and deployment of new technologies and scientific discoveries devolve from the relationships among pertinent agencies and their communication and cooperation patterns. These are taken up in this section.

3.3.1 Cooperation difficulties with R&D partners

Different kinds of Science and Technology entities are vital to the DOD enterprise, and they need to be able to work closely and effectively together:

> In an age of budget challenges and exploding technology, DOD cannot operate in seclusion. The Department has to make effective use of all available resources. Private industry, outside labs, and a variety of partners all help enhance the DOD mission…
>
> The strength of the Defense S&T program depends directly on the health of its partners. These partners together provide the environment that supports the needs of the warfighter. Each partner plays a vital role. Universities provide new ideas and knowledge, Service laboratories provide stability and ties to the

> operational forces, and DARPA is committed to high-risk, high-payoff programs. Other agencies allow us to leverage our combined resources. Industry provides innovation and transition of technology. Our international allies for joint research programs address interoperability from the beginning. Our S&T program is stronger because of these partnerships, each of which brings something unique to the solution of national security problems. (Etter, 2002, pp. 179-181)

The need for coordination and collaboration in science and technology is made more imperative by the complex, dynamic, interdependent, and often surprising nature of modern military operations, especially the now-prevalent Stability, Security, Transition, and Reconstruction (SSTR) Operations.

Derived from MOOTWs (Military Operations Other than War), and Civil-Military Operations Centers (CMOCs), SSTR Operations involving the military are now part of DOD doctrine and progressively comprise greater portions of U.S. military activity (Miles, 2005). Such operations require the expertise, access, and resources of many different kinds of organizations in the reconstruction of societies, in the aftermath of or in the midst of, war, catastrophe, or national failure. Department of Defense doctrine specifies that they are to be granted the same levels of importance, training, resources, and scientific support as “combat operations.” (DOD Directive, 2005). One might argue that increasingly they *are* the new form of military combat operations.

It is assumed that these operations will involve the interdependency and interoperability of many diverse organizations. A DOD directive states that in addition to the adversary, the following players should be assumed to be part of any large-scale SSTR Operation (in various combinations):

- -Department of Defense Components
- -Other U.S. Agencies and Departments (e.g., the State Dept., via USAID)
- -Foreign governments and their security forces (as in coalition operations)
- -IOs, International Organizations (e.g., the World Health Organization)
- -NGOs, Non Governmental Organizations (e.g., Doctors Without Borders)
- The private sector (for-profit companies, e.g., Bechtel) (DOD Directive, p. 3)

Such diversity accentuates the challenges of coordination, safety, cultural clash, and effective (*co*)operation. These new realities are reflected in the following sample of statements:

> The expanding role of combatant commanders in the international arena necessitates greater interagency linkages. The concept of full spectrum dominance in Joint Vision 2020, especially in the context of military operations other than war (MOOTW), must recognize that the intermingling of humanitarian assistance, combat operations, and nation building is indicative of future responses to security challenges. (Kelleher, p. 1)

> Joint Pub 3-0, Doctrine for Joint Operations, outlines the requirement for an integrated and coordinated response: Joint force commanders should ensure that their joint operations are integrated and synchronized in time, space, and purpose with the actions of other military force (multinational operations) and nonmilitary organizations (government organizations such as the U.S. Agency for International Development, nongovernmental organizations (NGOs), and the U.N.). (Kelleher 2002, p. 2)

Despite such calls for greater synergy, interagency conflicts still exist, even at the most basic levels, involving policy, processes, information sharing, and responsibilities:

> More than four years after September 11, the nation still lacks government wide policies and processes to help agencies integrate the myriad of ongoing efforts, including the agency initiatives we identified, to improve the sharing of terrorism-related information that is critical to protecting our homeland. Responsibility for creating these policies and processes shifted initially from the White House to the Office of Management and Budget (OMB), and then to the Department of Homeland Security (DHS), but none has yet completed the task. (GAO06, 2006, p. ii)

3.3.2 Problems associated with agency interdependency

Studies have been conducted regarding interagency operations and their effectiveness. One common critique centers on conditions of overlap of function and fragmentation; however, closer to the objectives of our project, there is also a recurrent theme of ineffective coordination and sharing of information, often related to policy and culture (e.g., GAO00, 2000). That is, sometimes barriers and incentives can result from the interdependency of agencies, through relationships of interdependent action and duties, oversight of one by another, conflicting regulations, and so forth. Very basic interoperability clashes can also hinder. For example: “Other critical stumbling blocks to interagency coordination are incompatible procedures, processes, data, and computer systems” (GAO00, 2000, p. 12). One might add differences in terminology, in classifications systems for information, inconsistency of interpretations of applicability of rules, and inconsistency in how many and what kinds of staff are entitled to make certain kinds of important security designations (GAO06, 2006, pp. 5-6).

One important example of *oversight* among agencies is that between the NSA and the military labs, in which the NSA has oversight responsibilities regarding national security in relation to information exchange and product release involving the laboratories (http://www.nsa.gov/ia/industry/tempest.cfm). Also regarding interaction and working together, barriers to *information exchange* across agencies, so called Cross-Department Information Exchange (CDIX) problems have been chronic, and show little sign of abating (e.g., Dillon, 2002).

Another significant problem is “stove-piping,” in which information acquired by one agency is propagated vertically to the top of that agency before being shared horizontally, usually as reports, with any other agency (e.g., Zinni & Koltz, 2006, pp. 130-142). This maladaptive practice is perpetuated because it helps maintain turf while generating evidence that the agency's processes are needed. One IC colleague, interviewed for this project, related, from personal experience, how a past President of the United States requested a newly created video tape of a public speech from another agency, and, at first, the agency refused to release it until they had "processed" it. Such practices preclude collaboration across agencies among rungs lower in the hierarchies of the organizations than the tops. This not only hampers timely, unfiltered information sharing, but more importantly precludes true cross-agency *collaboration*, in which professionals at the lower processing levels of the different organizations can think and discuss cases together, contributing their diverse perspectives about what information-*in-the-process* of analysis might *mean*.

3.3.3 Problems involving interagency competition

Different groups involved in the R&D process, while in many ways cooperative, sometimes compete for programs, funding, and access. This is particularly true across the services. As we have noted, as a result of this problem, groups may not communicate, coordinate, and collaborate with each other effectively or sufficiently. There is also competition for scarce resources, and this often leads to "turf protection," as groups try to bolster the idea that they are needed. Scarce resources include people. For example, there is an inadequate number of systems engineers within DOD (and this has contributed, for example, to the cancellation the Navy's Littoral Combat program in 2007; Charette, 2008, p. 36). Yet, the speed and variation of new kinds of warfare calls for ever-greater need for interagency cooperation, teamwork, and expertise:

> As the Armed Forces learned in Desert One, interservice rivalry leads to failure. The global war on terrorism and the summons by the President to synchronize instruments of national power comprise a watershed for breaking down barriers. Interagency coordination must be improved for the United States to continue its dominant role across a range of military operations. The opportunity to sow the seeds of interagency cooperation should not be missed. (Kelleher, 2002, p. 7)

An example of such interagency conflict is reflected in a GAO study of the problems of interagency conflict—in that *another affected agency questioned GAO's authority even to conduct such a study*:

> To provide for information-sharing policies and procedures, GAO recommends that the Director of National Intelligence (DNI) assess progress, address barriers, and propose changes, and that OMB work with agencies on policies, procedures, and controls to help achieve more accountability. OMB said that once ODNI completed its work, OMB would work with ODNI and all agencies on additional steps, if needed. *ODNI declined to comment on our report, indicating that the subject matter is outside GAO's purview.* We disagree with this assessment because it does not accurately reflect the scope of GAO's statutory authorities. (GAO06, 2006, p. ii, emphasis ours)

3.3.4 Current efforts to address barriers to interorganizational synergy

Measures are being developed to try to organize and coordinate the response of multiple agencies to the growing complexities they face. This includes the DOD S&T *Reliance* program. It seeks answers not only to overlaps in the activities of agencies, but also for greater opportunities and means for cooperation and synergy:

> The Defense S&T *Reliance* process includes a coordinating body that helps eliminate unnecessary duplication and seeks out opportunities for synergy, integrating the various component programs into a corporate S&T program. Reliance enables the DOD S&T community to work together to enhance S&T's role in supporting the Department's acquisition programs as well as the warfighters. (Etter 2001, p. 173).

Another response to this problem is the growing trend for government agencies to state their yearly contractual objectives in term of *outcomes* goals, rather than just *activities*. This is partly a result of the 1993 Government Performance and Results Act (GPRA). There is an expectation that if achievement of goals is demanded, and if these require collaboration to achieve, then agencies will work together in necessary ways. Simply contracting for activities leaves open the possibility that these will be addressed totally in-house.

> In the United States, GPRA is a key part of the legislative framework for shifting the focus of the federal government from a preoccupation with activities to results. GPRA requires the President to include with his annual budget submission a federal government performance plan. Congress intended this plan to provide a "single cohesive picture of the annual performance goals for the fiscal year." Under the Act, executive branch departments and agencies are to prepare multiyear strategic plans and annual performance plans. The Act also requires agencies to submit annual program performance reports… (GAO00, 2000, p. 4; see also GAO00, 2000, p. 3)

Along with outcomes-based planning and evaluation, other recommendations for greater cooperation follow fairly standard patterns, e.g., providing new mechanisms and oversight for coordination, alignment of goals, and so forth:

> …we have offered various specific approaches—such as setting up interagency coordination mechanisms, integrating service delivery, and consolidating programs—for rationalizing crosscutting programs. (GAO00, 2000, p.19)

3.4 Conflicting Requirements for Legality, Security, and Effectiveness

Throughout the long history of acquisitions, there has been a tension between expediency in meeting soldiers' needs, and being able to ensure safety, legality, and effectiveness of the materials ultimately provided (McNaugher, 1989). Even as there are now calls for greater openness, cooperation, and collaboration, there is concern that ever-increasing security restrictions and fears of broaching regulations are impeding the ability of the

R&D scientists to conduct their work. The sorts of restrictions cited by pertinent professionals we have consulted include:

- Restricted access to networks and information sources
- Restricted access to activities and resources pertinent to the R&D process
- Reduced freedom of action and interaction among scientists across government labs and with outside research organizations
- Restrictions concerning where and how scientists can conduct their work (e.g., not being able to carry or access their tools and materials for work at home)
- Restrictions in working with international students, scientists, and with ideas of foreign origin (Jacobs, 2004)
- Difficulties in accessing classified material due to increasing volume and inconsistencies in labeling:

> In the current environment, still affected by the long shadow of the terrorist attacks of September 11, 2001, several issues have arisen regarding security classified and controlled information. Volume is a concern: eight million new classification actions in 2001 jumped to fourteen million new actions in 2005, while the quantity of declassified pages dropped from 100 million in 2001 to 29 million in 2005…. Critically evaluating this activity, ISOO has indicated that the federal government needs to apply a more integrated approach among the classifying agencies. The force of, and authority for, information control markings, other than security classification labels, have come under congressional scrutiny, prompting concerns about their number, variety, lack of underlying managerial regimes, and effects. Among those effects, contend the Government Accountability Office and the manager of the Information Sharing Environment for the intelligence community, is the obstruction of information sharing across the federal government and with state and local governments. (Relyea, 2008, abstract)

3.5 Barriers Associated with Closed Systems and Hyper-Caution

In order to gain insight and provide guidance in designing our impending survey instrument, in addition to reviewing literature we have also had conversations with a small number of personnel in the intelligence and Army laboratory communities. The following are some resulting observations:

- All five individuals talked about a kind of extreme cautiousness that has overcome operators because of security and legal concerns. They expressed concern that “Security is so tight that no work is getting done,” or, alternatively, “people are reluctant to do anything” that might be found to infringe on security concerns.

- There is a concern that authorities are over-interpreting the rules, not even allowing things that are allowed within the rules. They are erring on the side of compliance.
- People are falling back to an extreme "logic of appropriateness" rather than a "logic of consequence" (March, 1978, 1989a, b). The tendency in such an approach is to make sure to dot every "i" and cross each "t" at one's own desk, rather than thinking about the impact of their decisions on the wider good.
- Provisions in E.O. 1333 and the Fourth Amendment dealing with "reasonable expectation of privacy" must be revisited in light of new realities. The consequence of current policies is essentially that lay people using Google have more access to some information than do analysts.
- The TEMPEST (NSA) certification process is a major obstacle to development and implementation of new technologies. Especially constraining is that testing and evaluation with actual or realistic analogue sources is prohibited until after certification is acquired.
- Across the sixteen different intelligence "silos," there in no common collaboration tool, though there are some current efforts that may show promise.
- There is still an "industrial assembly line" model of information processing that stifles across-person and across-agency collaboration, and reinforces and promotes "stove-piping." Incentives reward personal contributions more than collaboration.
- There is a concern that legal personnel are incentivized to "bullet-proofing" practices rather than enacting sensible and workable policies of risk-management.
- Release of sensitive but perishable information in response to urgent needs (e.g., welfare of the tactical warfighters) is too slow, if not impossible. Current procedures requiring manual release of such information need to be enhanced by automated or semi-automated computer assistance. New "policy-based information exchange" research is being directed toward this end (e.g., Bradshaw *et al.*, 2008; Bunch, *et al.*, 2008).
- While there is some *sharing* of the lowest levels of data across agencies, stove-piping precludes real *collaboration* in the interpretation of information at intermediate levels of analysis across agencies.
- Partly to protect tuff and maintain stove-piping, there is over-use of the ORCON designation—"origination of control."

Some of these have been discussed already. We now examine barriers noted above that are associated with extreme caution. We turn next, more generally, to this phenomenon and how it occurs within organizations. We start with "laws of fear."

3.5.1 Laws of fear

The goal of building and deploying new multi-component systems that can safely, reliably, and punctually deliver information to the soldier will be a daunting task, as we have seen from this review. It will require new ways and new flexibility. It will require new or adjusted policy, cooperation across multiple agencies, greater integration among these, and high degrees of net-centricity. However at just the time when new, and perhaps potentially riskier, thinking is so necessary, practitioners and institutions have become risk aversive, as we have outlined above. What has led to this cautionary stance, at this particular time? Among other factors, practitioners have pointed to some highly public oversight investigations that at times have shed agencies and operators in quite public, negative light (e.g., 9/11 Commission, Weapons of Mass Destruction Commission). People have become fearful.

In addressing similar issues of risk aversiveness, Sunstein defines fear as a "judgment that we are in danger" (Sunstein, 2005, p. 3):

> This book is about fear, democracy, rationality, and the law. Sometimes people are fearful when they ought not to be, and sometimes they are fearless when they should be frightened. In democratic nations, the law responds to people's fears… " Risk panics" play a large role in groups, cities, and even nations. (Sunstein, 2005, p. 1)

Risk panics develop in a people. They can be founded or unfounded. Democratic institutions must account to the people, but they also have a responsibility to ally myths and overreactions (as well as to "call to arms" when necessary). In this they should count heavily on pertinent expertise and science when these exist (Sunstein, 2005, *deliberative democracy,* pp. 1-2; Dekker, 2007). Institutions should also pitch policy at levels below the highly philosophical, value laden levels, if possible, especially when there are many, discordant stakeholders (e.g., avoiding deep issues of basic fairness, freedom regarding climate control or genetically-engineered food). They should concentrate more on practice and on the facts (e.g. famine), on how people conduct their lives and work, areas in which it might be easier to find agreement (Sunstein, 2005, *incompletely theorized agreements,* p. 2).

3.5.2 Risk aversion and the precautionary principle

The Precautionary Principle (PP) basically states that if there is the most minuscule chance that something terrible might happen from an action, one should create a policy to prohibit it (Sunstein, 2005, p. 5-6). Extreme precautions of this sort have been the subject of discussion in such highly sensitive areas as climate control, genetic engineering, and the recent start-up of the CERN particle accelerator (EONC, 2008).

Sunstein has noted two basic fallacies regarding the application of the PP. First, it fails to account for the fact that not taking action is also an action, with its own set of possible risks (for example, treating a patient versus "letting nature take its course"). Second, it is part of human perception that vivid (as regarding a possible catastrophe) or recent images (e.g., a highly publicized one) of a possible outcome can inflate people's probability estimation for such an event (Sunstein, 2005, p. 5; also Kahneman & Tversky, 2000). In this sense, the situations in which particular individuals and groups will exercise the Precautionary Principle can be idiosyncratic: i.e., cognitive but also cultural (Douglas & Wildavsky, 1982; Sunstein, 2005, p. 5).

Influences on fear and associated social "risk panics" include *social cascades, group polarization, and the "disaster myth."* Social cascades involve fear being passed from person to person, a kind of contagion. Group polarization has to do with the phenomenon in which groups, collectively, can come to hold more extreme views than their individual members (Sunstein, 2005, p. 6). The disaster myth is a phenomenon that has emerged in the news media, in which media emphasize the most dramatic incidents (Tierney *et al.*, 2006).

Two other sources of inaction and hyper-caution are *sunk costs* and *policy gridlock*. The first stems from how organizations have been doing things "for a long time," "the way we've *always* done it." Many stakeholders have benefited from "the old way," through positions attained, the skills required, known patterns of predictability and reward, and so forth. There will be elements of "pushback" with any substantial change, including policy change, about how things are to be done (McNaugher, 1989; Feltovich, Bradshaw, Clancey, & Johnson, 2007—regarding inertia within *"That which exists now"*). Policy gridlock emerges when stakeholders are so distant in their views on an issue that no coalition has the power to act on its own, and no progress can be made (Sunstein, 2005).

It has been proposed that beneath these fear-induced inertias just discussed are at least two common core factors: misjudgments of probabilities of adverse events and inflated views of the consequences of those events. We will briefly note four of these (following Sunstein, 2005, p. 35):

- The *Availability Heuristic*: Recent events trump long term trends. Vivid/dramatic examples override benign ones. Hence if there has been a recent, highly public type of disaster or *faux pas* (e.g., gross embarrassment resulting from a high-level congressional hearing), people will raise their expectations of that kind of event happening again
- *Probability Neglect*: Worst cases dominate in decision making (even if highly improbable)
- *Loss aversion*: People would rather keep what they have, rather than possibly losing it (sometimes related to "sunk costs," considerable effort that people have already expended)
- *Belief in the benevolence of nature*: The belief that not acting is safer than acting ("Things will play out ok."). This does not take into consideration that "not acting," itself is an action with its own potential risks as well as rewards.

All these factors, lending to fear of dire consequences for individuals and groups, contribute to the tendency for people and institutions to "hunker down," "play things safe," and only do things " by-the-book," even when the context argues otherwise. Such a stance has been labeled the "logic of appropriateness." The personal advantage of this approach is that if bad things happen, people can defend their actions by saying "I did exactly what I was supposed to." This stance may function effectively much of the time, but is often found wanting for unusual situations, problem situations crossing organizational and job description boundaries, interdependent activities, and so forth. In such cases, what is more urgently needed is a "logic of consequences," tailoring processes more flexibly to desired outcomes (March, 1978, 1989a, b). Like some recent government episodes (WMD, 9/11), other organizations have experienced hyper-caution and intense self-study after a series of highly public and much criticized “black-eyes.” Notable are medicine (Kohn, *et al*., 1999), nuclear power, and disaster response (Davis, *et al.*, 2007).

Do people and organizations have a right to be scared? Yes, embarrassing and damaging consequences have resulted from actions taken by agencies, both to the people and the organizations. But is there a rational basis for less fear? We have noted earlier that a large part of the fear results from conceptually faulty estimates of probably and consequences of untoward events. For instance, in a series of Washington, DC sniper attacks, it was discovered that *driving* to Baltimore to get gas, because many of the murders had been happening at local gas stations, actually had higher risk than gassing locally (Sunstein, 2005, p. 90-91). Anything that science and research can bring to making these estimates more realistic enables the employment of some form of cost-benefit analysis. Short of that ability, there are heuristics that may be employed to provide some protection, for instance:

- *Anti-catastrophe Principle*: Avoid options with the worst worst-case scenarios. Choose ones with best worst-cases (Sunstein, 2005, p.109-115).
- *Irreversibility Principle*: Choose actions with reversible consequences over ones that are irreversible (Sunstein, 2005, p. 58-59). And rare events, even very rare ones, do happen. There should always be plans in place if these occur, even though they may never have to be used.

We address additional approaches in the following sections.

3.5.3 Wicked problems and high reliability organizations

Many of the enterprises addressed in this report, such as military acquisitions and CDIX, deal with what have come to be called Wicked Problems (Rittel & Webber, 1973). Such problems tend to have the following properties (after Camillus, 2008, p.3):

- The problem can be framed, construed in many different ways.
- It is hard or impossible to decide when the problem has been “solved.”
- Evaluation of the quality of an option can only be accomplished over time.
- Any solution attempt is a one-shot-deal, and can’t be repeated (or undone).
- There are many possible solution options, not just one or a few.
- It is often hard even to determine which option is better.
- Every Wicked Problem is essentially unique because its fine particulars matter.
- Any such problem has many interactions with others and cannot be compartmentalized.
- Many different kinds of stakeholders care about the problem, and they may construe both solution paths and outcomes very differently.
- Outcomes have high impact; there are great consequences of being “wrong.”

Some of the industries we have mentioned (e.g., medicine, nuclear power, aviation) that can be said to deal with Wicked Problems have been found to benefit from instituting principles of "High-Reliability Organizations." HROs have been described thus:

> HROs are organizations with systems in place that are exceptionally consistent in accomplishing their goals and avoiding potentially catastrophic errors. The industries first to embrace HRO concepts were those in which past failures had led to catastrophic consequences: airplane crashes, nuclear reactor meltdowns, and other such disasters. These industries found it essential to identify weak danger signals and to respond to these signals strongly so that system functioning could be maintained and disasters could be avoided. (Hines, Lofthus, *et al.*, 2008, p.1)

Organizations that can benefit from adopting principles of HRO have been described as having the following kinds features, many of which are similar to those of Wicked Problems (after Hines, Lofthus, et al., 2008, p. 1):

- *Hypercomplexity.* There are complex environments with multiple teams and systems, presenting challenging coordination issues.
- *Tight coupling.* The actions of the parties and systems are highly *interdependent*.
- *Hierarchical differentiation.* There are clearly differentiated roles and reporting lines**.**
- *Multiple decision makers in the communication networks.* Many stakeholders and different kinds of stakeholders are involved in decisions, requiring open communications and negotiation.
- *High accountability.* Mistakes and bad decisions have high consequences.
- *Need for frequent, immediate feedback.* There is need for constantly monitoring of the functioning of the systems so that errors can be detected before they happen, mitigated when they do happen, and learned from after the fact.
- *Compressed timeframe.* Things happen fast and can change fast.

What has been found generally about these kinds of organizations is that closed operations (e.g., highly compartmentalized, secretive, punitive) are ineffective, dangerous operations, for both consumers (e.g., patients in medicine, operators in the intelligence community) and producers (e.g, medical providers, intelligence producers). Complex organizations that have been able to improve their safety and quality of service have instituted principles of High Reliability. These include:

- *A General Oversight Body*: There is some body in charge of setting standards for safe and effective practice, monitoring the conduct of these, and conducting research and education for continual system wide improvement (Kohn, Corrigan, & Donaldson, 1999, p. 6).

- *Constructive Treatment of Errors and Near Misses*: Rather than focusing on blame and repercussion when adverse events occur, errors, near misses and warnings from practitioners must be treated as opportunities to learn and improve for the whole organization (e.g., Kohn, Corrigan, & Donaldson, 1999, p. 4-5, 7; see also Hines, Luna, & Lofthus *et al.*, 2008, p. 16, *Just Culture*). This also involves *not oversimplifying* the causes of error, recognizing that notable failures usually have multiple and complex systemic causes (Feltovich, Hoffman, Woods, & Roesler, 2004; Hines, Luna, & Lofthus et al., 2008, p. 7). For example, the diagnosis of highly localized human error is tidy and convenient, but it is very often highly reductive of the reality (Dekker, 2007; Woods & Hollnagel, 2006, p. 111).

- *More Effective Communication, Transparency, and Feedback:* There should be continual monitoring and feedback concerning of the state of functioning of the entire system. As stated regarding medicine:

  > How well people and organizations make safety depends on feedback to recognize systemic vulnerabilities, to evaluate the robustness of their adaptations and to understand how the changing context of medical practice affects vulnerabilities. Recognizing systemic vulnerabilities guides investments to cope with these contributors toward failure. *Promoting this flow of information to learn about systemic vulnerabilities is one of the hallmarks of a safety culture.* (Cook, Woods, & Miller, 1998, p. viii, emphasis ours)

  In addition, to the extent possible and safe, the nature of processing and decision-making within units should be predictable, observable, and mutually directable by others, to deal with inevitable error correction and changing circumstances (Klein, Feltovich, Bradshaw, & Woods, 2004).

- *Cooperation and Collaboration*: The tight coupling of problems with other problems, their multidisciplinary nature, their many facets requiring different kinds of expertise, and the diversity and often strongly held views and appraisals of numerous stakeholders, require disparate parties to work together and seek workable understandings (e.g., Woods & Hollnagel, 2006, p. 182). Both tools and facilitation procedures for navigating conflicting views have been a major focus of the Wicked Problems movement (e.g., Conklin, 2006). Effective collaboration also at times requires linking particularly challenging aspects of work to those most qualified to help (i.e., particular experts), sometimes in contrast to official organizational structure or standard procedures (Dekker, 2007; Hines, Luna, & Lofthus *et al*., 2008, p. 9).

- *Standardization of Processes and Definitions:* Clearly, successful cooperation is made easier when interacting organizations have compatible classification schemes, technologies, and ways of doing business (Hines, Luna, & Lofthus, *et al.*, p.13-14; Kohn, Corrigan, & Donaldson, p.12).

- *Evaluate and Compensate for Desired Attitudes and Behaviors***:** If people are to freely report near misses, mistakes, and vulnerabilities, they cannot be punished for doing so (e.g., Dekker, 2007). Rather, they need to be encouraged and even rewarded. Also, if we want practitioners and different groups to share and collaborate, we cannot base performance evaluation for promotion, future funding, etc., solely on *individual procedures performed*, even though establishing quality metrics for joint and group activity, as well as associated accountability, is more difficult. Ultimately, evaluation and compensation are the "tails that wag the dog" of work-a-day practice.

In February 2008, the office of the Director of National Intelligence released a program for a new way of doing business. Its key focus was on information sharing and collaboration within and across organizations. As stated:

> Information sharing is a key element in the Intelligence Community’s transformation to provide better support for our Nation’s protection. The major factors driving the need for change are the changing threat environment, new national and homeland security customers, and emerging threats that require synthesizing intelligence from a greater variety of sources. (DNI, 2008, p. 5)

Many of the envisioned changes are much in line with proposed remedies for dealing with Wicked Problems and High-Reliability Organizations that we have reviewed, for instance in the aspects of a designated head, sharing, collaboration, more openness, greater standardization where possible, and the need for revised “cultures” and policies. These have been shown in other industries to lead to better and safer operations, both for the organizations applying them and for the practitioners within them. For example, they make transactions more public, dispersed, and multi-sourced—alleviating somewhat the liability of individual units:

> The 9/11 Commission Report: Emphasizes the need to *change the mindset from “need-to-know” to “need to share.”* Moreover, it places *the DNI as the principal change agent* in creating a culture within the Intelligence Community focused on data “stewardship” rather than data “ownership.” The 9/11 Commission challenges the concepts of “originator controlled” (ORCON) adopted by collectors, which inhibits information dissemination and sharing and creates *diffused information ownership and inconsistent access standards*. (DNI, 2008, p. 6, emphasis ours)
>
> Meeting these needs requires development of a culture that *values sharing information* with those who need it, and providing them with the *training, policies, laws, processes, and information* technologies necessary to distribute their knowledge (DNI, 2008, p. 7, emphasis ours)
>
> True information sharing ensures that all participants in the intelligence cycle supporting collection, analysis, dissemination, and feedback have the information they need when they need it. Members of the Intelligence

> Community must be able to discover the existence of information and retrieve relevant information when needed. Analytic organizations supporting senior decision makers must have the means to understand the implications of the most sensitive information when creating a product. The information itself must be available through an accessible Intelligence Community infrastructure that supports *information discovery, retrieval, and collaboration:* (DNI, 2008, p. 10, emphasis ours)

The document also addresses the critical need to *support and reward* practice, attitudes, and behaviors that support the new ways of operation:

> *Developing a Culture that Rewards Information Sharing is Central to Changing Behaviors…* Changing the culture to one that naturally encourages the responsible sharing of information is fundamental to success. Training must increase the emphasis on the "responsibility to provide" while understanding the implications of the protection of sources and methods, privacy, and civil liberties within that responsibility. If Intelligence Community personnel perceive that their professional success is based in part on how well they share information, sharing will improve (DNI, 2008, p. 11, emphasis ours)

3.5.4 Current efforts to address barriers due to closed systems and hyper-caution

As of the middle of 2009, the oversight body charged to monitor the transition from "need to know" to "responsibility to share," has reported to congress three times, the last in May, 2009. Of the many objectives involved in making the transition, the body reported greatest progress on training and training materials, development of sharing policies within agencies, attempts at standardization of policies and procedures, and initial attempts at creating evaluation and reward structures for sharing (ISE08, p. 48; see also McNamara, 2008). With regard to actual shared practice, there has been progress in the development of "fusion centers," local and state multi-agency intelligence centers, and the "information sharing environment," fundamental infrastructure to support the enterprise (ISE09).

In a different vein, since the directive for greater openness itself came from the DNI, there are interesting questions about how compliance will roll out across the different agencies since, when the DNI itself was established, this had differential effects on the status and operations of the agencies that had existed before DNI. It cannot be assumed that everybody is happy with the ascendance of the Office of the Director of National Intelligence and with their own subsequent changes in duties, prestige, and operations.

4 Summary

There are many issues involved in the process of fielding new ideas and technologies to operational use. Most of these are longstanding and have defied numerous attempts at amelioration, even swinging back and forth from one pole to another across time and across more or less successful implementations. The acquisition process itself is like this.

Unresponsiveness and speed have always been prime issues. Various approaches for accelerating the process have been tried as experiments, and some such experiments are being tested today (e.g., the Urgent Universal Need Statement—UUNS; MARADMIN, 2006). The results are being evaluated.

The key loci for idea creation, development, testing, and so forth, have repeatedly swung between the government venues and outside contractors. Initiative may lie primarily with the government agencies, until various factors like manpower, expertise, and funding demand that more of the effort needs to me outsourced to contractors. Contractors then rule, until a perception emerges that they may be "fleecing the American taxpayer," taking advantage of their positions, or acting inefficiently or deviously. Then the pendulum swings back. This cycle has been going on for a long time (McNaugher, 1989), and at present the power seems to be edging back to the private sector contractors (Charette, 2008).

Where the R&D process takes and tests its ideas has had very similar swings, from the offsite research labs or from the field of battle. At present, because of exigencies of war, there is greater focus for close contact with soldiers' needs. In fact, needs for quick, flexible adaptation to changing enemy tactics and technologies has spawned great creativity and resourcefulness among the soldiers themselves, for example in armoring their vehicles and improvising functional communication systems. Inter-service and interagency rivalries have also always played a part, partly because of competition for resources and duties, partly to maintain the perception of being indispensable, and partly because of engrained institutional histories and cultures. Finally, there has always been a tension between delivering a needed tool in a timely way, versus delivering the "perfect" tool, totally tested, reliable, i.e., "bullet-proof." The paradox in this is that by the time such an ideal tool can come to fruition, the world has changed, the enemy, not thus constrained, has long before created an effective albeit perhaps flawed device, components and replacement parts are no longer available for the "better" device, and so forth. Finally, the press for speed in deliverables may at times be at odds with the pursuit of longer term, basic science research, and this has always been the case.

All these issues have become more critical and complex in the current world. This is a world of speed, change, connectivity, global reach, high technology, rouge social groups, and fluid, sometimes seemingly capricious "rules." The nexus of these challenges present a picture much in line with what have come to be called "Wicked Problems," for instance in the difficulty of measuring progress, let alone success, across the many and diverse stakeholders, and in the complex interdependence of components. Such factors have, more or less successfully, been confronted in other industries (e.g., nuclear power, aviation, medicine) through adoption of "high reliability" principles. Among these are greater adaptability, openness, collaboration, stakeholder involvement and planning, the engagement of expertise, diligence in monitoring operations, constructive learning from mistakes, and incentives for adopting high reliability practices such as reporting near misses (and errors) and actively working with other pertinent parties. New overtures within DOD and the military seem headed in this kind of direction (e.g., Charette, 2008; Conklin, 2006; DNI, 2008; Etter, 2001; Gates, 2009; Petraeus, 2006). A global example of trying to address large-scale Wicked Problems more generally, in public policy, is that of the Australian Public Service (AUS, 2007). The challenge is to make these kinds of efforts succeed, through technology development, policy, practices, incentives, support, and evaluation and promotion structures that are consistent with the aims, or that at least do not subvert them (Dekker, 2007).

5 References

(AUS07). (2007). *Tackling wicked problems: A public policy perspective.* Contemporary Government Challenges, Australian Public Service Commission.

Bernsten, R. & Pezzullo, R. (2005). *Jawbreaker.* New York: Crown Publishers.

Bradshaw, J. M., Hoffman, M., Just, J., & Bennett, M. (2003). Policy management overview. Invited presentation and white paper deliverd to the DARPA Information Awareness Office at the Genoa II policy management workshop, Arlington, VA, 27 March.

Bradshaw, J. M., Beautement, P., Breedy, M., Bunch, L., Drakunov, S. V., Feltovich, P. J., Hoffman, R. R., Jeffers, R., Johnson, M., Kulkarni, S., Lott, J., Raj, A., Suri, N., & Uszok, A. (2004). Making agents acceptable to people. In N. Zhong and J. Liu (Eds.), *Intelligent Technologies for Information Analysis: Advances in Agents, Data Mining, and Statistical Learning*, Berlin: Springer Verlag, pp, 361-400.

Bradshaw, J. M., Feltovich, P. & Bunch, L. (2008). New research directions in policy-based information exchange. *Tactical Cross-Domain Policy Workshop,* Army Research Laboratory at Adelphi, 10 September 2008.

Bunch, L., Bradshaw, J. M. & Young, C. O. (2008). Policy-governed information exchange in a US Army operational scenario. Demonstration track. *2008 IEEE Conference on Policy,* Palisades, NY, 2-4 June.

Camillus, J.C. (2008). Strategy as a wicked problem, *Harvard Business Review*, May, 1-10.

Charette, R.N. (Nov., 2008). What‘s wrong with weapons acquisitions? *IEEE Spectrum, 45*(11), 32-39.

Conklin, J. (2006). *Dialogue Mapping: Building Shared Understanding of Wicked Problems*. New York: Wiley.

Davis, L.E., Rough, J., Ceccine, G., Gareban-Schaefer, A., Zeman, L.L. (2007). *Hurricane*
Katrina: Lessons for Army Planning and Operations. Rand Corporation, Santa Monica

Dekker, S.D. (2007). *Just culture: Balancing safety and accountability.* Hampshire, UK: Ashgate Publishing.

(DNI) (Feb., 2008). *U.S. Intelligence Community: Information Sharing Strategy.* Office of the Director of National Intelligence.

(DOD Directive) *Military Support for Stability, Security, Transition, and Reconstruction (SSTR) Operations* (2005). Department of Defense Directive No. 3000.05, November 28, 2005.

Douglas, M., & Wildavsky, A. (1982). *Risk and Culture: An Essay on the Selection of Technological and Environmental Dangers.* Berkeley and Los Angeles, CA: University of California Press.

(DSB01). *Defense Science Board 2001 Summer Study on Defense Science and Technology.* Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics. May, 2002.

(DSB06) *Defense Science Board 2006 Summer Study on 21st Century Strategic*

Technology Vectors. Volume IV. Accelerating the Transition of Technologies into U.S. Capabilities. Office of the Secretary of Defense, April 2007.

(DSB07). *Report of the Defense Science Board Task Force on Strategic Communication*. Office of the Secretary of Defense, April 2007.

Dillon, D.R. (2002). *Breaking Down Intelligence Barriers for Homeland Security*. Heritage Foundation, Backgrounder #1536, April.

(EONR) (2008). *The safety of the LHC*. Report by the European Organization for Nuclear Research, http://public.web.cern.ch/public/en/LHC/Safety-en.html

Etter, D.M. (2001). Defense Science and Technology. In *26th Annual AAAS Colloquium on Science and Technology Policy*. Washington, DC.

Feltovich, P.J., Bradshaw, J.M., Clancey, W.J., & Johnson, M. (2007). Toward and Ontology of Regulation: Socially-Based Support for Coordination in Human and Machine Joint Activity. In *Engineering Societies for the Agents World VII*, edited by G. O'Hare, et al. Heidelberg, Germany: Springer-Verlag.

Feltovich, P.J., Hoffman, R.R.,Woods, D., & Roesler, A. (May-June, 2004). Keeping it too simple: How the reductive tendency affects cognitive engineering. *IEEE Intelligent Systems*, 90-94.

Flanagan, J. L., Huang, T. S., Jones, P. and Kasif, S. (1997, July). "Final Report of the National Science Foundation Workshop on Human-Centered Systems: Information, Interactively, and Intelligence (HCS)." Beckman Institute for Advanced Science and Technology, University of Illinois at Urbana-Champaign.

Gates, R.M. (2009). A balanced strategy: Reprogramming the Pentagon for a new age. *Foreign Affairs*, Jan/Feb, 28-40.

(GAO00). (2000). Managing for results: Barriers to interagency cooperation. GAO: Report to the Honorable Fred Thompson, Chairman, Committee on Governmental Affairs, U.S. Senate. GAO/GGD-00-106. March.

(GAO05). (2005). *Defense technology development: Management process can be strengthened for new technology transition programs.* GAO: Report to congressional committees, June.

(GAO06). (2006). *INFORMATION SHARING: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information.* Report to Congressional Requesters, GAO-06-385, March.

(GAO07). (2007). *DEFENSE ACQUISITIONS: Future Combat System Risks Underscore the Importance of Oversight.* Testimony before the Subcommittee on Air and Land Forces, Committee on Armed Services, House of Representatives, GAO-07-672T, March.

Gerding, E.F. (2006). The next epidemic: Bubbles and the growth and decay of securities regulation. *Connecticut Law Review, 38*, pp. 393-453.

Hines S, Luna, K, Lofthus J, et al. (April, 2008). *Becoming a High Reliability Organization: Operational Advice for Hospital Leaders.* (Prepared by the Lewin Group under Contract No. 290-04-0011.) AHRQ Publication No. 08-0022. Rockville, MD: Agency for Healthcare Research and Quality.

Hoffman, R. R., Ford, K. M., and Coffey, J. W. (2000). "The Handbook of Human-Centered Computing." Report, Institute for Human and Machine Cognition, University of West Florida, Pensacola FL.

Hoffman, R.R., & Elm, W.C. (2006). HCC implications for the procurement process. *IEEE Intelligent Systems, 21*(1), 74-81.

(ISE08), June, 2008. *Annual report to the congress on the information sharing environment.* Prepared by the Program Manager, Information Sharing Environment.

(ISE09), May, 2009. *Annual report to the congress on the information sharing environment.* Prepared by the Program Manager, Information Sharing Environment.

Jacobs, L.L., Deputy Assistant Secretary of State for Visa Services (2004). *The Conflict Between Science and Security in Visa Policy: Status and Next Steps.* Testimony before the House of Representatives Science Committee, Washington, DC, February 25.

Kahneman, D. & Tversky, A. (2000). Prospect theory: An analysis of decision under risk. In D. Kahneman & A. Tversky (Eds.), *Choices, values and frames*. Cambridge UK: Cambridge University Press.

Kelleher, P.N. (2002). Crossing boundaries: interagency cooperation and the military. *Joint Force Quarterly*, Autumn Issue.

Klein, G., Feltovich, P.J., Bradshaw, J.M., & Woods, D. D. (2005). Common ground and coordination in joint activity. In W.R. Rouse & K.B. Boff (Eds.), *Organizational simulation*. New York: Wiley.

(MARADMIN) (2006). *Urgent universal need statement process (UUNS)*. No. 045/06, 1-26-06)

March, James G. "Bounded rationality, ambiguity, and the engineering of choice." *The Bell Journal of Economics 9*, no. 2 (1978): 587-608.

March, James G. *Decisions and Organizations*. Blackwell Publishers, 1989.

March, James G. *Rediscovering Institutions*. Free Press, 1989.

McNamara, T.E. (2008). Information sharing guidance : Inclusion of information sharing elements in employee performance appraisals (ISE-G-105).

McNaugher, T.L. (1989). *New weapons, old politics.* Washington, DC: Brookings Institute.

Miles, D. (2005). *Defense Science Board Report Recommends New Focus on Stabilization, Reconstruction.* American Forces Press Service, Washington, Jan. 25, 2005.

Neville, K., Hoffman, R.R., Linde, C., Elm, W.C., & Fowlkes, J., (2008). The procurement woes revisited. *IEEE Intelligent Systems*, *23*(1), 72-75.

(OFT05). (2005). *The Implementation of Network-Centric Warfare*. Office of Force Transformation, Office of the Secretary of Defense, 1000 Defense Pentagon, Washington, DC 20301-1000, Jan. 5.

Petraeus, David H. (2006). Learning Counter Insurgency: Observations from Soldiering in Iraq. *Military Review*. On the web at: http://usacac.army.mil/CAC/milreview/English/JanFeb06/Petraeus1.pdf

Relyea, H.C. (2008). *Security Classified and Controlled Information: History, Status, and Emerging Management Issues.* CRS Report for Congress, AAAS Center for Science, Technology and Security Policy, Order Code RL33494.

Rittel, H.J.W., & Webber, M.M. (1973). Dilemmas in a general theory of planning. Policy Sciences, xxxx

Stephenson, J. (2007). *Losing the golden hour: An insider's view of Iraq's reconstruction*. Washington DC: Potomac Books.

Schacht, W.H. (2007). Technology Transfer: Use of Federally Funded Research and Development. CRS Report for Congress, Order Code RL33527, July, 19.

(Sentatus): *Daily coverage of the United States Senate*, February 18, 2008.

Sunstein, C. R. (2005). *Laws of fear: Beyond the precautionary principle*. Cambridge, UK: Cambridge University Press.

Tierney, K.J., Lindell, M.K., & Perry, R.W. (2006). Facing the unexpected: Disaster preparedness and response in the United States. Washington, DC : John Henry Press.

Whittaker, Alan G., Smith, Frederick C., & McKune, Elizabeth (2007). *The National Security Policy Process: The National Security Council and Interagency System*. (Research Report, April 2007 Annual Update). Washington, D.C.: Industrial College of the Armed Forces, National Defense University, U.S. Department of Defense.

Zinni, T., & Koltz, T. (2006). *The battle for peace: A frontline vision of America‘s power and purpose.* New York: Palgrave-Macmillan.