Defense Science Board
Task Force

on

The Role and Status of DoD Red Teaming Activities

September 2003

Office of the Under Secretary of Defense
For Acquisition, Technology, and Logistics
Washington, D.C. 20301-3140

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
SEP 2003	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Defense Science Board Task Force on The Role and Status of DoD Red Teaming Activities	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Office of the Undersecretary of Defense For Acquisition, Technology, and Logistics Washington, DC 20301-3140**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**48**	

This report is a product of the Defense Science Board (DSB).

The DSB is a Federal Advisory Committee established to provide independent advice to the Secretary of Defense. Statements, opinions, conclusions and recommendations in this report do not necessarily represent the official position of the Department of Defense.

This report is UNCLASSIFIED

OFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON, DC 20301-3140

DEFENSE SCIENCE
BOARD

MEMORANDUM FOR ACTING UNDER SECRETARY OF DEFENSE
(ACQUISITION, TECHNOLOGY & LOGISTICS)

SUBJECT: Final Report of the Defense Science Board (DSB) Task Force on the Role and Status of DoD Red Teaming Activities

I am pleased to forward the final report of the DSB Task Force on the Role and Status of DoD Red Teaming Activities. Transforming the capabilities of an organization requires adept use of the tools of management. Red teams can be a powerful tool to understand risks and increase options. However, the record of use of red teams in DoD is mixed at best.

The attached report identifies several types of red teams and examines some current red team activities in DoD. Drawing on red team experience in government and the commercial sector, the report identifies obstacles and suggests criteria for their effective use. It recommends specific issues that would benefit from red teaming and also steps that the Secretary of Defense should take to make red teaming a more effective tool throughout the Department.

I endorse all the Task Force's recommendations and propose that you review the Task Force Chairmen's letter and report.

William Schneider, Jr.
Chairman

OFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON, DC 20301-3140

DEFENSE SCIENCE
BOARD

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Final Report of the Defense Science Board Task Force on the Role and Status of DoD Red Teaming Activities

This report addresses how red teams can help DoD transform. We define red teams broadly, including not only playing the adversary, but also playing devil's advocate and related roles. While differing in some respects, these activities all have in common the challenging of an organization's norms. Thus red teaming at its essence is about the culture of an organization.

We believe red teaming is especially important now. Adversaries are tough targets for intelligence. Red teaming can both complement and inform intelligence collection and analysis. Aggressive red teams challenge emerging operational concepts in order to discover weaknesses before real adversaries do. Red teaming also tempers the complacency that often follows success.

To address these problems we recommend that the Secretary of Defense establish a few red teams in critical areas and take steps to inculcate effective red team use throughout the department.

We suggest several areas for increased red teaming. We believe none is more important than helping understand the military lessons that others (adversaries and possible suppliers of capabilities to adversaries) will garner from Enduring Freedom, Iraqi Freedom and other recent US military operations. We recommend starting with perhaps a half dozen or so subject nations (and sub national entities) spanning a range of motivations and capabilities and for each address their possible responses at the strategic, operational and tactical levels.

Our recommendations to instill effective red teaming in the Department include developing and distributing a red teaming best practices guide and making the subject of red teaming an intellectual endeavor to be researched and taught at the institutions of professional military education.

We thank the task force members and government advisors for their efforts and contributions. We also thank our Defense Science Board Secretariat representatives and support staff, particularly LTC Scott Dolgoff and Ted Stump.

Ted Gold

Bob Hermann

TABLE OF CONTENTS

I. INTRODUCTION

The Task Force was charged to examine the use of red teams in the Department of Defense and recommend ways that such teams could be of greater value to the department. Our Terms of Reference and task force membership are provided in Appendices 1 and 2.

Our usage of the term red team includes not only "playing" adversaries or competitors, but also serving as devil's advocates, offering alternative interpretations (team B) and otherwise challenging established thinking within an enterprise.

We argue that red teaming is especially important now for the DoD. Current adversaries are tougher targets for intelligence than was the United State's major cold war foe. Red teaming deepens understanding of options available to adaptive adversaries and both complements and informs intelligence collection and analysis. Aggressive red teams are needed to challenge emerging operational concepts in order to discover weaknesses before real adversaries do. In addition, in the wake of recent military operations, use of red teams can temper the complacency that often follows success.

Chapter II elaborates on what we mean by red teams and red teaming. The attributes of effective red teams are discussed in Chapter III. A summary of some current red team activities in DoD is provided in Chapter IV. Chapter V and Appendix 3 discuss a special case of the use of red teams where the red team addresses issues fundamental to the existence of the enterprise and not just particular plans or programs. Conclusions and recommendations are offered in Chapters VI and VII. A draft Secretary of Defense memorandum implementing our recommendations is provided in Appendix 5. Appendix 4 contains historical examples of red team activities, and finally, there is a glossary provided in Appendix 6.

II. WHAT ARE RED TEAMS AND RED TEAMING?

Red teams and red teaming processes have long been used as tools by the management of both government and commercial enterprises. Their purpose is to reduce an enterprise's risks and increase its opportunities.

Red teams come in many varieties and there are different views about what constitutes a red team. We take an expanded view and include a diversity of activities that, while differing in some ways, share a fundamental feature.

Red teams are established by an enterprise to challenge aspects of that very enterprise's plans, programs, assumptions, etc. It is this aspect of deliberate challenge that distinguishes red teaming from other management tools although the boundary is not a sharp one. (There are many tools used by management for a variety of related purposes: to promulgate visions, foster innovation, promote efficiencies.)

Red teaming can be used at multiple levels within the enterprise; for example, at the

- Strategic level to challenge assumptions and visions,
- Operational level to challenge force postures, a commander's war plan and acquisition portfolios,
- Tactical level to challenge military units in training or programs in development.

In general, red team challenges can help hedge against surprise, particularly catastrophic surprises. It does this by providing a

- Wider and deeper understanding of potential adversary options and behavior that can expose potential vulnerabilities in our strategies, postures, plans, programs, and concepts. This role (to explore technically feasible and responsive threats) has become increasingly important as a complement to the more traditional intelligence-based threat projections (capabilities-based versus threat-based planning).

- Hedge against the social comfort of "the accepted assumptions and the accepted solutions". This includes hedge against bias and conflict of interest.
- Hedge against inexperience (a not uncommon situation in DoD and other Government Agencies where leadership tenures tend to be short).

Areas where red teams can and do play an important role within DoD include:

- Training
- Concept development and experimentation (not just an OPFOR for the experiment but continuous challenge by red teams throughout the concept development process)
- Security of complex networks and systems
- Activities where there is not much opportunity to try things out (for example, nuclear weapons stockpile issues)

A red team is comprised of individuals selected for their special subject matter expertise, perspective (professional, cultural), imagination or penchant for critical analysis. Members of the team could be from within or outside the organization, their assignment to the team could be temporary or extended and the team itself can be of short-term duration or standing. In some rare cases, the culture of the enterprise fosters challenge to the degree that it acts as its own red team.

The red team itself is only one element in a red teaming process. The process can be explicit or ad hoc. Elements of the process include the following: who the red team reports to; how it interacts with the management of the enterprise and with "blue" (the owner of the activity it is challenging), and how the enterprise considers and uses its products.

We identify three types of red teams. Our expanded notion of red teams includes teams established to serve as:

- Surrogate adversaries and competitors of the enterprise,
- Devil's advocates,

- Sources of judgment independent of the enterprise's "normal" processes (often from team members with experience from positions at higher levels in industry or government).

Surrogate adversaries and competitors: This category itself includes a wide range of activities. The purpose of these red teams is to sharpen skills, expose vulnerabilities that adversaries might exploit and in general increase understanding of the options and responses available to adversaries and competitors.

In some, the team tries to emulate an adversary or competitor. The setting could be a military training, experimentation or gaming environment where the red team plays the "Opposing Force", using the adversary's presumed tactics and equipage (actual or virtual). Examples in the training arena are the Army's OPFOR at the NTC and the JRTC, the Air Force's at Nellis AFB and the Navy's at Fallon and Key West.

The setting could also be red team attacks to compromise an information or computer system. The setting for the surrogate adversary could be future acquisition – where a red team might – under conditions similar to those available to the adversary—invent counters to US military systems.

In some cases the red team is not explicitly constrained to think and behave as an adversary might, but is given wider latitudes to discover technological counters to US systems. A successful example of this type of red team (and one of the longest established red team processes in DoD) is the Navy's Subsurface Ballistic Nuclear (SSBN) Security Program.

Devil's advocate: These red teams offer critiques of, and in some cases alternatives to, the enterprise's assumptions, strategies, plans, concepts, programs, projects and processes. At the program level the objective of this type of red team is to provide critical analysis in order to anticipate problems and avoid surprises. The red team's subject, either explicit or implicit, can also be process, how an organization conducts its business. An example of such a team was the Ballistic Missile Threat Committee that Secretary Rumsfeld chaired in 1998. It examined the same data available to the intelligence community but identified alternative paths adversaries might take and came to different conclusions about the threat.

General Advisory Boards and other sources of independent judgment: The objective is often to be a sounding board and "kitchen cabinet" for the sponsor.

III. WHAT MAKES AN EFFECTIVE RED TEAM?

Red teaming is important but it is not easy nor often done very well. The Task Force looked at red team experiences within and outside of DoD and concluded that there are formidable challenges to establishing and sustaining effective red teams and associated red teaming processes. Meeting these challenges involves to a large part managing the tradeoff between independence and interaction. Typical causes of red team failure include the following.

The red team:

- Does not take its assignment seriously (Task force members commented that in their own experience serving on red teams they rarely were provided with a clear statement of objective).
- Could lose its independence and be "captured" by the bureaucracy (or could be self inflicted by the red team trying to figure out what the sponsor really wants).
- Could be too removed from the decision making process and thus become marginalized.
- Could have inadequate interaction with "blue" (i.e., the program or activity it is challenging) and be viewed as just another sideline critic. (DoD doesn't need to pay for these; there are plenty out there).
- Could destroy the integrity of the process and lose the confidence of decision makers by "leaking" its finding to outsiders.

There are additional challenges for red teaming that provide surrogate adversaries including:

- Not capturing the culture of the adversary / competitor (but instead mirror images).

- Quality of red team insufficient to provide interesting challenges to "blue" (perhaps because of resource constraints on red).

ATTRIBUTES OF EFFECTIVE RED TEAMING

With the challenges of the previous section in mind we offer the following as basic ingredients of successful red teaming.

The culture of the enterprise: This may be the most important contributor to effective red teaming. Red teaming can thrive in an environment that not only tolerates, but values internal criticism and challenge. Unfortunately, it is often the case that those organizations in need of red teaming have a culture inimical to its use.

Top Cover: A red team needs a scope, charter and reporting relationship that fit the management structure. A red team should be expected to raise issues that might not be welcome throughout the enterprise; it needs the support, sometimes from the very top levels of the enterprise. Top cover is needed to ensure that the red team's products not only have the requisite degree of independence, but are seriously considered as well (this does not imply acceptance). Two related attributes are:

1. **Independence with accountability:** The independence to avoid becoming subordinate to the programs it is challenging, accountability to make it relevant and timely and to maintain the integrity and confidentiality of the process.
2. **A process in which the output of the red team is seriously considered and can be acted upon in a timely manner:** Without such a process, red teams become marginalized or merely another sideline critic.

Robust interaction between the red and "blue" teams: It is not a win or lose game. The objective is to establish a win-win environment in which blue learns from the process and comes out with sharper skills or more robust solutions and / or greater appreciation for the issues that their superior must deal with. When the red team is charted to offer alternative

solutions it is important to incentivize them to challenge basic assumptions and get to the root issues.

Unusually careful selection of staff: Success of any activity depends on proper staffing. Staffing red teams present special challenges. Many very talented individuals are not necessarily suited, temperamentally or motivationally to be effective red team members. Furthermore, resource constraints normally imposed on red teams necessitate judicious selection of the right mix of talents and perspectives. Imagination is a particularly desirable attribute. Most members of the team will not be permanent red teamers and selection can also be based on the potential for professional development. Red team members often regard the experience as the best training they have had.

A deft touch in the use of red teams: Too often, red teams will be called for only after major problems have arisen or after too many resources have been expended when an earlier use of red teams could have anticipated the problems and changing directions been less painful. However, if used too early, with too heavy a hand, promising ideas may be prejudged as failures.

IV. Observations About Current Red Team Activities

US Navy's SSBN Security Program: This red team activity has had an extraordinary long life. The program was established in the early 1970s to identify potential vulnerabilities that the Soviet Union might exploit to put US SSBNs at risk. This program, by identifying potential vulnerabilities in the SSBN force, also had a "shadow" customer in the Navy's own antisubmarine warfare programs.

Originally established to look at the vulnerabilities of the US SSBNs, the focus of the program shifted in the mid 1980's to evaluate and assess findings from the intelligence community. Recent work has involved SSBN protection vulnerabilities, terrorist threats, and security in port. The perspective on SSBN survivability changed as well over time with the

collapse of the Soviet Union and the advent of new asymmetric threats. In the 1970's and 1980's, the objective for SSBN survivability was hours (sufficient to deter a nuclear exchange). After the cold war ended, the survivability came to be viewed in terms of days or months.

Though the scope and focus of the SSBN Security Program has changed over the decades, its guiding principles have remained largely unchanged and have been a major factor in the Navy's ability to sustain an effective program for so long. These principles include:

- Strong and widely acknowledged national purpose
- Stable and adequate funding
- Highly competent people
- Access to the details of the target program (vital for this effort, in general the level of access can be a control variable in red teaming)
- Independence to criticize
- Direct accountability to senior official (outside of the SSBN program management line) empowered to take corrective action
- A strong, but not subordinate, relationship with the Intelligence community

The SSBN Security Program assesses threats and vulnerabilities based on physical principles and thus represents one form of red teaming. These assessments are determined by technological feasibility and operational realities, not on cultural differences or other geopolitical considerations.

Missile Defense Agency - Red Teaming Experience: For almost two decades the Missile Defense Agency (MDA) and its two predecessor organizations, the Strategic Defense Initiative Organization and the Ballistic Missile Defense Organization, have employed a variety of red team techniques. The purpose of these activities has been to identify, characterize, understand and mitigate the risk associated with the development and deployment of a missile defense system.

They have used several types of red teams. In one (sometimes characterized as threat-based) the main purpose is to understand responsive countermeasures. These red teams typically do not interact much at all with

blue. The products of this kind of red team are typically descriptions of suites of penetration aids that an adversary might design and deploy (in the near, mid or far-term) in response to a US missile defense system. These products are generally reflected in "evaluate-to" threats which tend to have little programmatic impact compared to the intelligence-based "design-to" threats.

In contrast to this "threat based" approach is a second type of red teaming effort ("capability based"). The primary emphasis of these red teams is to understand the capabilities and susceptibilities of the blue missile defense system in order to exploit inherent weaknesses in the blue system. The red team is typically as interested in blue assumptions about the threat as it is in actual blue capability. This form of red teaming requires a continuous and detailed exchange of information between the red and blue teams. It is our impression that in spite of good intentions, this type of red teaming has been difficult to achieve and sustain. The current MDA director has attempted to facilitate an intimate red and blue interaction by focusing the red team effort on certain critical issues and by using a high profile white team to foster significant interchange between the red and blue teams.

Red team membership has been drawn from a variety of sources over the years including Federally Funded Research and Development Centers, intelligence agencies, National Laboratories, defense contractors as well as small numbers of people from the missile defense organizations themselves. US citizenship has typically been a requirement for membership. However, MDA currently has a red team composed solely of UK citizens whose purpose is to understand as much as they can about the US missile defense system from unclassified US sources as well as all foreign sources but without having direct contact with US blue components.

Individuals on red teams usually have had a strong technical background. For one long-running red team, however, membership specifically was limited to individuals without special technical expertise or knowledge about missile defense countermeasures. This activity -- the Countermeasures Hands-On Program (CHOP) -- was established by SDIO over ten years ago in response to a 1992 Defense Science Board Task Force on SDI Countermeasures. The Task Force's concern was the possibility that

relatively unsophisticated countermeasures were not being adequately addressed.

Since CHOP was established at Kirtland Air Force Base in Albuquerque NM, over a dozen “skunk work” missions have been completed. Typically the participants (different for each mission) are about half a dozen young military officers and government civilians (with recent engineering degrees). They are not given any classified information about the blue system. In each mission they are given a countermeasure related problem and are then asked to identify, design and often, actually build, countermeasures to US defense systems. They exploit commercial computer programs, standard machine tools and commercial electronics. In several cases the countermeasures they built, some subscale, have been demonstrated in actual flight tests. In spite of these successful experiments, it is not clear to this Task Force whether the program has had much impact on the missile defense program.

Given the highly public and controversial nature of the subject, the missile defense organizations have received much “free red teaming” from non-government and government sources. MIT Professor T. Postol’s analysis of photographic and other evidence on Patriot intercepts during the 1991 Gulf War and April 2000 Union of Concerned Scientists report, "Countermeasures: A Technical Evaluation of the Operational Effectiveness of the Planned US National Missile Defense System" are examples of the first.

Perhaps the external red team effort that has had the greatest effect on the management of the missile defense program was the 1998 report of the “Commission to Assess the Ballistic Missile Threat to the United States”. This effort was created by congressional legislation in the Fiscal Year 1997 National Defense Appropriations Act and chaired by Mr. D. Rumsfeld (then a former secretary of defense). This study helped to foster the organizational acceptance of subsequent red team analyses, liberating it from the bonds of standard intelligence assessments, which are typically based on relatively straightforward and limited extrapolations of what had actually been seen.

Air Force Red Team Program: The Air Force Directorate of Electronics and Special Programs is home to the Air Force Red Team program

(SAF/AQLR). The Air Force Red Team provides assessments of concepts and technology (as opposed to serving as a surrogate adversary). The Red Team's scope spans the entire Air Force and it has the funding and authority to conduct analyses and design and perform field tests. Their process involves making judgments (in part based on open literature) about capabilities and knowledge of future adversaries. They also involve the Intel community in the process, to get input from this community and also to provide feedback to help inform intelligence collection and analysis about what to look for if an adversary attempts to achieve a new capability.

Their process involves red/blue interaction in order to evaluate and recommend blue system improvements. They argue their approach:

- Provides disciplined approach to guide decision making in technology development
- Allows warning regarding vulnerability of fielded capabilities
- Gives insight into defining what sensitive information to protect

A measure of red team success is when their data has altered a development plan or an acquisition program (e.g., initial production was limited; subsequent upgrade produced a better product).

From their experience, attributes of an effective red team include independence from the project offices, experienced personnel, constructive environment (i.e., recommend blue force improvements as counter countermeasures), and a capability to evaluate the art of the possible (i.e., looking at risk based on technical possibilities, not just known capabilities).

The US Army's Red Franchise Organization: The US Army in 1999 established a Red Franchise organization within its Training and Doctrine Command (TRADOC) to guide Army training, concept and force development, experimentation, and transformation.. The Red Franchise organization is responsible for defining the Operational Environment for the next two decades, which is defined in Joint Publication 1.02 as "the composite of all conditions, circumstances and influences which affect the employment of military forces and bear on the decisions of the unit commander." The Operational Environment is the intellectual foundation for transforming the Army from a threat-based force to the capabilities-

based Objective Force. The Operational Environment is more useful than specific threats to guide force development and support spiral development.

The Red Franchise organization (reporting to TRADOC DCSINT) has a great deal of independence from its customers in TRADOC and in the joint and interagency communities. Its products, including the Joint Operational Environment (written in partnership with U.S. Joint Forces Command – USJFCOM) and threat portrayals, are used to support wargames and experiments concept development. The Red Franchise provides its products to other Services, and Joint and interagency customers as well. The Red Franchise also have produced an "instruction manual" for the Opposing Forces (OPFOR) at the Joint National Training Center (JNTC), the JRTC and the CMTC in which they provide guidance on the composition and behavior of opposing forces. The Red Franchise makes heavy use of outside experts to develop their products.

TRADOC has more recently stood up the Devils Advocate organization separate from but able to support the Red Franchise as necessary or appropriate with the mission to support Army and DoD/Joint transformation by conducting and coordinating studies, reviews, and analysis of concepts, requirements documents, and training products. The Devil's Advocate places particular attention to the Army's Objective force, the Future Combat System, and related initiatives.

USJFCOM Red Teams for joint concept development and experimentation: JFCOM has been using red teams for joint concept development (including Rapid Decisive and Effects-Based Operations) and experimentation (including Unified Vision '01, Millennium Challenge '02 (MC02) and Unified Quest '03).

JFCOM representatives to our task force stated a continuing need to get red teams engaged earlier in the concept development and experiment design process before large amounts of money (and therefore egos / careers) are committed to a concept. They cited a need for standards for establishing and using red teams for joint concept development and experimentation and organizational self-confidence to accept and act on criticism. Understanding the difference between an experiment and an exercise is important. Concepts can fail; experiments fail only if nothing is learned.

The challenge of using red teams effectively in experiments was highlighted by concerns expressed by the person that played the OPFOR commander in MC02. MC02 was billed as an experiment that would allow the OPFOR a measure of free play (and we understand would also document when and why red team play was constrained and the lessons learned and follow-up analysis needed). Instead MC02 was more demonstration than experiment, involving an orchestration of events that precluded free play.

OSD's Defense Adaptive Red Team (DART) Activity: The DART was established by the Deputy Under Secretary of Defense (Advanced Systems and Concepts) in June 2001. Its mission is to support the development of new joint operational concepts by providing red teaming services to JFCOM, the combatant commands, Advanced Concept Technology Demonstration (ACTD), Joint Staff, and OSD. The services run the gamut of red team types. They include serving as surrogate adversaries for wargames and experiments; conducting vulnerability / failure analysis for concepts (e.g., ONA and RDO); doing Team B development of competing concepts; providing an independent assessment of experiments (UV01 and MC02); and providing a framework for concept development and evaluation for the joint staff. It also is identifying best practices in red teaming.

Based on their experience, DART emphasized several lessons about necessary conditions for effective red teaming:

- Support from the top, which is a combatant commander for most of their customers,
- Support and active involvement from people in the organization that can make things happen, and
- Trust at all levels, and appropriate confidentiality since the red team is raising fundamental issues about how organizations conduct their business.

V. Red Teams At The Strategic Level

A special case of red teaming occurs when the entire enterprise is challenged (rather than a project or product). A more detailed discussion of

the differences between the two cases is provided in Appendix 3. The role of a strong red team can be especially important when the enterprise's CEO or Senior Executive or Officer faces the following:

- Change is urgent, but what to do is unclear; e.g., regulatory change
- CEO can't order the change due to lack of credibility; e.g., non-technical executive in a scientific, medical, or craft organization
- Change required is so abrupt that buy-in by a majority of the power 'barons' is required; e.g., in a University, Military, Religion.
- Resistance is strong / immediate or long-lasting / subversive; e.g..discriminatory practices, labor problems.
- CEO has a short tenure due to age or practice.
- Pervasive change is required in decision-making, financial control, career paths, and organizational power / turf, which cut across existing organizational boundaries.

When these conditions exist, the CEO needs to find a good solution that can be implemented, is hard to reverse, and will continue whether or not he / she is in charge.

The role of the red team in such a situation is to:

1. Clarify the degree of urgency of the threat / required change. Provide factual, balanced analysis, objective if possible, to their peers for debate and discussion (important that team members be credible).
2. Create alternatives backed by data, feasibility, likely outcome, difficulty of implementation, resources required, likely resistance, communication needs. Compare to existing, or momentum, approach. Challenge assumptions, myths, turf, beliefs.
3. Gather opposing views, and ensure they are communicated clearly. (Important since many people are reluctant to voice valid concerns.)
4. Lead discussions toward choice of an acceptable solution. "Acceptable" is defined by need, not political preference. Balancing what is needed versus what is feasible versus what is political takes

some skill. CEOs don't always take well solutions they don't like. The red team may or may not have a preferred solution.

5. Plan implementation, gathering views on difficult problems, identifying resources necessary, organizing communication and feedback

6. Project manage the onetime activities of the transition until the organization is able to do so. This could take several months.

7. Disband.

Significant change requires scores or hundreds of mini-projects in a large organization. At the beginning, few managers have the perspective on what is needed or what is possible. Most executives undertake a change of major magnitude only once in their careers at the top of the organization. A red team, reporting to the CEO, or perhaps the Executive Committee, can make a tremendous difference in how well change is accomplished. They often are the articulate advocates for change.

VI. CONCLUSIONS

Red teaming has long been a valuable, if underutilized, tool for the Department of Defense. The use of red teams has become especially critical now and we recommend that their role be expanded. There are two reasons:

1. **To deepen understanding of the adversaries the US now faces in the war on terrorism and in particular their capabilities and potential responses to US initiatives.** Red teaming to help identify the range of options available to potential adversaries (state and sub-state) using accessible technology and asymmetric means is an important complement to evidentiary based threat assessment from intelligence and other sources. Intelligence collection is also informed by red teaming and the insights it offers into possible threat actions and responses. We believe this complementary role has grown in importance because these adversaries present much more difficult targets to collect against than our cold war adversary, the USSR.

2. **To guard against complacency.** The US military is attempting to transform itself – the force that triumphed in Operation Iraqi Freedom fought quite differently than the force that prevailed in Desert Storm 12 years ago. Perhaps the most difficult environment to transform an enterprise is during a time of great success. It will however be necessary to continue transforming our armed forces to deal with committed and adaptive adversaries (perhaps much more so than faced in the recent operations). Aggressive and pervasive red teaming throughout DoD and particularly in OSD, can help avoid complacency and even more self-defeating attributes that too often are part of a victor's baggage.

The use of red teaming is expanding within DoD and the intelligence community, largely because of the first reason above – to help understand the new threats

However, the task force is concerned that because of the historical difficulties of creating and sustaining effective red team processes, many new initiatives to establish red teams will not provide the expected value.

Attention from the highest levels in the DoD will be necessary to establish and sustain quality red teams and red teaming processes. Effective red teaming will be much more influenced by a change in the culture of the enterprise than by attempts to institutionalize red teaming or putting someone in charge. Cultural change within DoD is a formidable, but feasible, task. It is underway, for example with respect to jointness as evidenced by the way US forces operated in Operation Iraqi Freedom.

VII. RECOMMENDATIONS

We have two. The SecDef should

1. **Take steps to inculcate effective red team use throughout the department**
2. **Establish a few red teams in critical areas.**

1. The SecDef should take the following steps to inculcate effective red teaming throughout DoD:

   - Issue a memorandum (draft provided in Appendix 5) that offers general guidance to the Department on the value of red teaming and directs specific actions to promulgate its more effective use. (This is a way to reach executives / leaders that he might not touch / influence directly).
   - Task the USD (AT&L) to outline the procedures to be used in the several forms of red teams and to develop a current best practice guideline for how to do red teams well. Make them widely available in the Department.
   - Make red teaming the subject of continuing intellectual activity at the PME and other relevant institutions. Teach it, research ways to do it better, keep abreast of red team activities (government and commercial, US and foreign). Idenfity successful red teamers to be the instructors in Professional Military Education (PME) courses. The PME courses themselves should be crafted around important Service, Joint, or OSD red team projects. Task the CJCS and the USD (AT&L) to be co-leads in making this happen.

2. The SecDef should establish red teams in a few critical areas

We believe most important is to establish a substantial red team effort to help understand the military lessons that others will garner from OEF, OIF and other recent US military operations. The focus should be on potential adversaries and suppliers of adversaries. The number of actors of interest can be quite large. We recommend starting with perhaps a half dozen or so subject nations (or sub national entities) spanning a range of motivations and capabilities. For each entity of interest we suggest that two teams be established: one to address strategic / operational responses, the other operational / tactical.

We recommend that the USD (P), USD (AT&L), USD (I) and the CJCS be assigned responsibilities for establishing and conducting these red team efforts. The intelligence community should participate strongly in this exercise but intelligence is but one input to understanding threat options.

Other candidates for more aggressive red team activity include:

- The nuclear weapons program and associated stockpile stewardship because of the inability to test the weapons
- Elusive targets (can learn from recent campaigns)
- Force projection process and its collaborating contributors including Regional Combatant Commands, TRANSCOM, JFCOM, DLA, etc (to improve capabilities in terms of agility, speed, reduced footprint)

Red teams could help enhance the way DoD approaches the development and fielding of networked capabilities and related systems-of systems (becoming more the norm). Red teams could also be used to more aggressively challenge evolving joint concept and prototypes. These are both opportunities to create multi-Service red teams within a joint context.

APPENDIX 1. TERMS OF REFERENCE

ACQUISITION, TECHNOLOGY AND LOGISTICS

THE UNDER SECRETARY OF DEFENSE

3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

14 FEB 2002

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Terms of reference—Defense Science Board Task Force on the Role and Status of DoD Red Teaming Activities

You are directed to establish a Task Force to review the role and status of Red Teaming in the DoD and recommend ways to make it a more effective tool. The review should encompass current and past Red Team activities within the DoD and its agencies as well as other government and non-government organizations (including those initiated since September 11).

Red Teaming can be a powerful tool to challenge conventional wisdom and wishful thinking within an organization. One form of red Teaming particularly important to national security is to serve as surrogate adversaries to contest our strategies, plans, concepts and programs. The intent is to make these strategies, plans, concepts and programs more robust and thus better able to deal with the real world's resourceful and adaptive adversaries.

Red teaming has long played an important role within DoD but the growing need for effective red teaming is highlighted by September 11 and subsequent events. We face new adversaries, employing asymmetric means. The militarily relevant technology base is increasingly commercial and globally available. The US itself is exploring new operational concepts that need to be "stressed" to the breaking point so we can learn their potential vulnerabilities before pitting them against real adversaries who will seek to exploit them. Since we are also moving to greater reliance on capability rather than threat-based planning, red teaming is even more vital for exploring the realm of technologically feasible, operationally feasible and responsive threats as a necessary complement to the evidentiary-based threat assessments provided by the intelligence community.

The TF should pay particular attention to addressing ways to overcome recurrent difficulties of conducting successful red team activities. These obstacles include:

- Capturing the thinking and motivation of adversaries with different cultural and social backgrounds, thus avoiding the tendency to "mirror image" our own thinking
- Preventing the Red Team from becoming co-opted by the advocates and managers of current policies, plans and programs

- Preventing the Red Team from becoming a mere sideline critic instead of interacting in constructive and creative ways with decision makers

The recommendations should be relevant to red teaming that portrays both state and non-state adversaries. It should also include how the DoD should work with other government Departments and Agencies to foster effective red teaming. The Task Force recommendations should address issues of red team products, processes and organization including but not limited to the following:

- What is an appropriate scope for red team activities? How many? What kind?
- How should they be staffed? Composition?
- To whom should they report?
- What types of products should be developed?
- How should their products be disseminated?
- How should product quality be ensured? Evaluated?

The Task Force will be co-sponsored by the Undersecretary of Defense (Acquisition, Technology and Logistics) and the Director, Strategic and Tactical Systems. Dr. Ted Gold and Dr. Bob Hermann will serve as the Task Force Chairmen. Mr. Chuck Sieber, S&TS, will serve as the Executive Secretary and LTC Carla Kendrick will serve as the Defense Science Board Secretariat representative.

The Task Force will be operated in accordance with the provisions of P.L. 92-463, the "Federal Advisory Committee Act," and DOD Directive 5105.4, the "DoD Federal Advisory Committee Management Program." It is not anticipated that this Task Force will need to go into any "particular matters" within the meaning of Section 208 of Title 18, U.S. Code, nor will it cause any member to be placed in the position of acting as a procurement official.

E. C. Aldridge, Jr.

APPENDIX 2. TASK FORCE MEMBERS

Task Force Co Chairman:

Dr. Theodore Gold
Dr. Robert Hermann

Task Force Members:

Dr Joseph Braddock
Mr Bran Ferren
Dr. John Foster, Jr.
Dr. Joseph Markowitz
Mr. Jack Welch, Jr.
Mr. William Delaney
Dr. Craig Fields
Dr. Ronald Kerber
Mr. John Stewart
Maj Gen Jasper Welch, USAF (Ret)

Executive Secretary:

Mr. Chuck Sieber, OSD Land Warfare

DSB Secretariat Representative:

LTC Carla Kendrick, USA, USD(AT&L)/DSB
LTC Scott Dolgoff, USA, USD(AT&L)/DSB

Government Advisors:

Dr. Theodore Barna, DUSD/AS&C
Mr. Shane Deichman, USJFCOM

APPENDIX 3. CONTRASTS BETWEEN PRODUCT/PROJECT AND ENTERPRISE RED TEAMS

Chapter V of the report refers to the special case of red teaming that occurs when the entire enterprise is challenged and not merely a project or product. The distinction among the types of red teams is significant in terms of the difficulties encountered in establishing and conducting effective red teams. When the focus of the red team is a process (instead of a project or product), the team attributes can be those of an enterprise red team. It would depend on how deeply and broadly the process is embedded in the the enterprise.

Specific attributes that help define the type of red team include:

- significance
- scope
- success / cost of failure
- executive sponsor
- assumptions
- tradeoffs
- mental framework
- team leader
- team composition, and project plan.

The table highlights differences in these attributes between program / project and enterprise red teams. It is followed by a description of some of the challenges to achieving these attributes in an enterprise red team.

Table 1. Characteristics of Product / Project and Enterprise Red Teams

ATTRIBUTE	PRODUCT/PROJECT TEAM	ENTERPRISE TEAM
SIGNIFICANCE	Important, urgent, not terminal to organization	Existence as a major player in jeopardy, perhaps over several years
SCOPE	1 program; less than 50% of enterprise	Affects >75% of enterprise; its place in larger world, what it is known for in the past
SUCCESS/COST OF FAILURE	Lower cost or time; better function or quality; may miss opportunity	Unknown for years; unclear; end of the enterprise is the risk
EXECUTIVE SPONSOR	Operating executive, program manager	CEO, Secretary, Board
ASSUMPTIONS	About design rules, cost, time, quality and their importance	Values; capacity to change; available leadership, will, skill, external trends
TRADEOFFS	Cost vs. Time vs. Function vs. Quality	Politics, power, history, risk of error, investment, people, current vs. future
MENTAL FRAMEWORK	Mission, objective, tradeoffs	External trends of economics, funding, competition, technology: internal values
TEAM LEADER	Good engineer, leader, manager	Strategic thinker, organizer, critical thinker
TEAM COMPOSITION	Engineers, finance, contracts, manufacturing, support	Executive, Planner, CFO, Political, Behavior, Technology trends (+same as project)
PROJECT PLAN	Specific, scheduled, followed	Unclear; blind alleys; exploratory
EXAMPLES	▪ Reduce cost/time in radar company. ▪ Ramp up production of Army helicopter. ▪ Build manufacturing facility in 50% of time. ▪ Increase ship building capacity from 5 to 6 per year. ▪ Start generic drug company. ▪ Increase hospital operating room capacity by 20% with no cost investment. ▪ Avoid $60M investment in power generation.	▪ Reduce drug lead time by 50%. ▪ Catch semiconductor industry leader within 2 generations. ▪ Accelerate automobile development from 6 to 3 years. ▪ Size steel industry (up or down) ▪ Merge or not defense electronics company ▪ Post Challenger upgrade manufacturing

Significance: Generally, an enterprise team is faced with either a major problem or a major opportunity, which will significantly alter the organization. The consequences are large but not necessarily immediate, which tends to delay addressing the situation.

Consequences for commercial companies can include a major loss of market share, missing a generation of technology, being 4th or 5th into a technology, being bought against its will, or bankruptcy. Consequences for government organizations can include major press embarrassment followed by house cleaning and damage to reputations of executives, loss of institutional influence, or program elimination. For some, the result is unfavorable combination with incompatible organizations.

Early recognition of significant consequences is an essential skill. But often, even those who see looming consequences fail to address the problem aggressively, such that they are managed by circumstances rather than manage circumstance. There are many commercial world examples: including in electronics, shipbuilding, steel, pharmaceuticals, electrical equipment, and automobiles.

Scope of Red Team: The scope of an enterprise red team is usually quite broad. It can encompass what is happening politically and economically around the world, how the organization's position is changing among its peers, how it is governed, and how the basic processes of management should change. New courses of action tend to be disruptive, advantaging some parts of the organization and disadvantaging others. Not infrequently, the senior leadership is the problem and must either change behavior or change jobs. Such outcomes pose a delicate communication challenge for the red team; senior executives vary widely in their response sometimes "killing the messenger" aka red team leader.

Success/Cost of Failure: Enterprise red teams tend to develop "solutions" or "roadmaps" which cannot be conclusively proved before the fact. Therefore, arguments can ensue and factions vie for a more convincing position. The red team leader and executive sponsor must clarify the cost of failure even if they cannot precisely define success (often it is easier to do the former). For example: "failure to develop the next generation

technology by X will result in our losing the entire Y market, even though we are not sure that the next generation of technology will be profitable"; or "unless test scores of students improve, we will lose control of the schools"; or "we don't know what success in anti-terrorism looks like, but we sure know what failure looks like." The role of the executive sponsor is far more extensive on these enterprise problems than on product/project problems.

Executive Sponsor: The executive sponsor for an enterprise red team has a tough task. The terms of reference to the team must be sufficiently broad, yet not so broad that it is impossible. He should not prejudice the team's thinking, but if he does, he must encourage disagreement (more about this below). He must pick a team matched to a task he has never done before. It is unlikely that he recognizes all the major issues or constraints. He is starting a process not defining an end product. Often there is opposition to starting the team.

Once started, the executive must strike balance after balance. He must encourage progress, but discourage superficial analysis; require new and useful facts but rein in analytical anarchy; challenge myths but preserve their truths; break down turf fences but tactfully; trample on other executives prerogatives but not with self-interest; question values but not their importance; sponsor ideas for change without demeaning past progress. It is not easy.

Throughout, informed dissent must be encouraged. This too can be easy. Junior people are uneasy disagreeing with senior people in groups larger than two (and sometimes one). Dissent sounds like criticism, and feels like criticism to some. A team member from engineering has trouble challenging the Chief Engineer, for whom he has worked (two levels down) and will once again work (more than two levels down). The sponsoring executive must encourage, goad, challenge, brow-beat other senior managers to do something that does not come naturally in hierarchies – allow and encourage dissent from the red team members and others.

In addition, the executive sponsor provides intellectual quality control and relevance to the team, although he is learning as they do, or even with a few weeks lag. Not easy. And it is not easy to recognize an answer. It is only possible to recognize the best available answer and judge whether it is sufficient. That is judgment of a high order.

Assumptions: This is a major stumbling block in enterprise red team activity. Wrong early assumptions cause failure. Assumptions must be sharply challenged, and challenged again. Statements such as "that is not feasible, it is outside our mandate, they won't stand for it, you can't be serious, or that will never happen" depress active challenge.

Less tangible, but still critical, assumptions are more difficult to challenge than tangible ones, and thus may not be routinely questioned. For example, "our product is better than their product" can be clearly challenged through reverse engineering and discussions with customers. "Their new product introduction process is giving them a real advantage over us" is less easy to prove. Yet, it was crucial in pharmaceuticals, autos, and mobile telephones with major adverse consequences to very good companies which awakened far too late.

Assumptions about human behavior particularly need challenge. "The union won't buy that, the Congress won't do that, our customers are too loyal to do that" need close examination since the most frequently repeated truisms are often only partially correct, and one can drive a truck through partially. It is more often true that "X will occur if new conditions A, B, C are created which are feasible though difficult." When creating an enterprise red team, this aspect deserves attention by the best minds available.

Within DoD, assumptions about cultural obstacles - " change will be too hard" or "take too long"-particularly need to be challenged. What is often characterized as a deep-seated cultural problem can turn out to be largely due to an absence of leadership and lack of widely perceived need.

Tradeoffs: Everyone knows how to make tradeoffs. Sometimes the specifics are hard but the process is well known in engineering and economics. However, enterprise red teams are usually unskilled at making the trade-offs that they face. For example, "alienating half of our customers to gain a new set of more desirable customers" is not typically a tradeoff taught in business school. "Risking leadership in the industry if we fail at risky venture X" faces few executives in their working career. Or for the British Cabinet, "shall we choose 1 billion pound sterling adverse trade balance, or 500 million pounds sterling operating loss, or lay off 50,000

Welsh steel makers two years before election?" is not part of the curriculum taught at Oxford or Cambridge

Unfamiliar tradeoffs require clarity of presentation in order to generate debate. Yet the temptation is to 'fuzz the issue' when it is uncomfortable, embarrassing to senior people or hard to clarify. The CEOs who keep pressing for clarity even when they are part of the problem will get better results for the organization and actually enhance their leadership and esteem.

Mental Framework: The mental framework for solving enterprise problems parallels the problems themselves. External information is preponderant. Outside trends in technology, economics, politics, finance, and competition are important. Internal value shifts, capacity and speed to change, current economic strength and weakness, awareness of people about the outside world, all affect how quickly major change can be accomplished. Forecasting is unfortunately necessary because medium and large organizations change very slowly and major change requires half a decade. However, finding red team members who are accustomed to thinking about half-decade change programs is not easy. R&D professionals are no better than others with the exception that they are usually very good at assessing technology rates of change.

Team Composition: As can be deduced from above, ideal team members are most likely nonexistant. The art is to mix quite different skills. Technology is often an issue; should an engineer, scientist, specialist, systems type, or futurist be the team member? And where do you find finance people who will be constructive, not obstructive when ideas obviously require lots of capital or losses or risk? Can behavior types stop facilitating the red team long enough to be analytically perceptive about trends in internal and external populations? And politics is about here and now, not two years from now no matter how important trends are. In other words, selecting individuals with skills can't be delegated. It is high-order handicraft.

Project Plan: The enterprise red team of course needs a plan, but flexibility must be an intrinsic part of the plan. Enterprise teams are somewhat like R&D – initial exploration of many avenues, triage of approaches and possibilities, digging deeper into a few and finally

concentrating on the very few that offer major opportunity. For example, in a UK steel example, balance of trade data did not exist in useful form, apparent pricing was quite different than real pricing (though strictly forbidden by policy), productivity data was not comparable and was, in fact, wrong, and competitors all assumed that they would increase market share of world steel to justify expansion plans even though everyone agreed on limited market size. A precise plan would have been useless almost as soon as it was written.

Perspective data, not financial accuracy is important initially. Teams cannot ask financial or IT departments for a particular analysis and wait for a result. The time required is too long, the accuracy specious, and perspective lacking.

APPENDIX 4. HISTORICAL EXAMPLES OF "RED TEAM" ACTIVITIES

The term "red teaming" as it is currently used is relatively new, but military organizations have utilized the types of activities encompassed by the phrase for quite some time. In particular, they have used war games with adaptive simulated enemies to test war plans, as well as emerging concepts. At a more rudimentary level, simply having a person (or group of people) look for vulnerabilities in plans, or offer alternative takes on scenarios, has proven of considerable value. Examining some historical case studies of such war games might be useful to see how games might best be used in the current environment, as well as to examine the misuses of red teaming methodologies.

EXAMPLES OF SUCCESSFUL RED TEAMS

German development of armored warfare in the Interwar Period. As a result of the Treaty of Versailles, Germany was unable to buy or build any kind of armored vehicles (other than police vehicles). But, the Germans were able to learn from the exercises being conducted by the British, who were at the forefront of tank development. Most importantly, they initiated a series of studies to look critically at the lessons of World War I in order to apply those lessons to emerging doctrine. As a part of that careful examination, the German military was able to conceptualize how armored forces might be utilized, as well as "how a potential opponent might utilize armor against German forces."[1] The insights developed by this series of studies was pivotal in the German conduct of the blitzkrieg.

US carrier aviation in the Interwar Period. The U.S. Naval War College conducted a series of war games that helped extrapolate technological trends in the strategic environment. While the contemporary level of technology at the time did not allow for the exploration of some questions, a series of war games conducted between 1923 and 1935 demonstrated the potential of aircraft carriers to act independently, which in turn affected

[1] Murray, Williamson. "Armored Warfare: The British, French and German Experiences" in Military Innovation in the Interwar Period. New York: Cambridge University Press, 1996. p.39.

decision-making about procurement. That level of insight eventually paid off for the U.S., because after Pearl Harbor, America possessed a carrier fleet to allow it to recover from the loss of its battleships. In fact, the raid at Pearl Harbor may have been the catalyst that the United States needed to force it to abandon the age-old "Battleship Paradigm" that placed primacy on the big gun and relegated the aircraft carrier to a supporting role.

Operation Post Mortem (June/July 1945). During the course of the war, the British had great difficulty in assessing the effectiveness of their ECM systems. In 1945, though, they captured intact the German air defense command in Denmark. In late June and early July the British decided to run full-scale, mock raid against the system to test the effectiveness of their ECM systems. The operation inherently had some artificiality. For example, there was no German fighter coverage employed; and, because the air defense system in Denmark had not been attacked during the war, it consisted mostly of inexperienced operators. Nevertheless, the British were able to gain valuable insights into the effectiveness of their systems.[2]

Cuban Missile Crisis (1962). On the first day of the crisis, October 16, President Kennedy organized the "Ex Comm" (the Executive Committee of the National Security Council) to help advise him on the situation, and U.S. responses to the unfolding crisis. His choice of those in the Ex Comm (especially his brother and the Attorney General, Robert Kennedy) was a deliberate move to provide alternatives for courses of action and act as a counterbalance for the strong military response, originally being advocated.

Another example of Kennedy's use of dissenting views to produce alternative courses of actions occurred on October 27. Early in the day, a letter had been received from Khrushchev. It was more formal than previous communications, and the tone indicated that someone might have written it other than Khrushchev. The State Department drafted a response that tried to answer some of the concerns raised, but there was dissent as to whether that was the correct way to go. Robert Kennedy and others (including Ted Sorenson, the Presidential Counsel) suggested ignoring that letter and answering the proposal made in the previous letter. Debate over the subject was heated, and in response, President Kennedy ordered Robert

[2] Rosen, Stephen Peter. Winning the Next War: Innovation and the Modern Military. Ithaca: Cornell University Press, 1991. p. 198.

Kennedy and Sorenson to go into another room to draft a counter-proposal. That allowed the President to look at the two choices and thus make a decision. In the end, the Kennedy / Sorenson draft was the letter the President signed and sent to Khrushchev.

EXAMPLES OF UNSUCCESSFUL RED TEAMS

Pearl Harbor (1941). In one respect, the war gaming surrounding the attack at Pearl Harbor was a success for the Japanese. As intended, the attack sank or disabled the majority of the U.S. Battleship fleet. And while there was disappointment that the U.S. carrier fleet was not present, and thus escaped unscathed, Japanese planning had focused on American battleships, not aircraft carriers.

On the other hand, Japanese planning for Pearl Harbor did not consider certain aspects that a thorough red team might have suggested. First of all, it never considered the impact that aircraft carriers would have on the course of the war. Even though the Pearl Harbor attack eventually led the demise of the "Battleship Paradigm", the Japanese still based their assumptions about the course of the war on the theory that surface warfare consisted of battle fleets engaging enemy battle fleets and relegated aircraft carriers to a support role.

Misdirected objectives of the raid are another issue not addressed by war gaming. If the Japanese had concentrated on attacking the military infrastructure (such as the harbor installation, workshops, dry docks, and oil storage facilities) instead of on the warships, the raid would have been more effective at delaying the American response. The Japanese did disable part of the U.S. fleet, but the infrastructure remained largely intact. Thus, the U.S. Navy was able to make a fast recovery. The harbor was still serviceable (and thus able to receive American aircraft carriers and prepare them for offensive operations), and equipment was mobilized to salvage and repair many of the ships sunk during the raid (making them available for offensive operations later in the war). Attacking the harbor infrastructure would have forced the American fleet to operate from West Coast bases. Even attacking the oil depots in Hawaii would have resulted in the laborious process of restocking fleet trains that would have required months to organize.[3] For all

[3] U.K. Ministry of Defense. War With Japan, Vol. II: Defensive Phase. London: HMSO, 1995. p. 25.

of 1942 the U.S. military would have had to use its West Coast bases rather than Hawaii for its military operations in the Pacific.

Japanese war plans also flawed in the strategic approach that the Pearl Harbor raid took, which was contrary to Japan's overall strategy. The goal of the attack was to destroy U.S. morale and force a compromise that accepted the situation in the Pacific. As one Japanese planner pointed out, "while a war which began with an attack in the south might be ended in a compromise, an attack on Pearl Harbor would destroy any hope of a compromise settlement."[4] The conception of the raid rested on the assumption that the U.S. fleet posed a threat to the Japanese flank in the event of a southward attack. But Japanese intelligence at the time knew that the U.S. fleet did not have the tankers or supply ships to support a flank attack.

Midway (1942). On May 1, 1942, the Japanese Combined Fleet Headquarters conducted a four-day series of war games to test the operations planned for Midway and beyond. The scope of the plans amazed some critical officers who noted that the formidable program "seemed to have been dreamed up with a great deal more imagination than regard for reality."[5] In hindsight, we know the Midway operation was a dismal failure. Looking at the details of the war game reveals flaws in the approach and philosophy that should be highlighted for the war planner of today.

First, even considering the scope and complexity of the operations, the war game rested on the assumption that the Imperial Navy could execute all operations without difficulty. In no small measure, this was due to the arbitrary interference of the officer presiding over the war game, Rear Admiral Ugaki, who set aside the ruling of the umpires when they adversely affected the Japanese side.

Second, the lack of familiarity with the plans by the operational commands responsible for the conduct of the war game resulted in those commands following the lead of the staff of the Combined Fleet Headquarters. In a telling example, a question arose as to how the First Carrier Striking Force (under Vice Admiral Nagumo) would react to an

[4] Weinberg, Gerhard. A Word At Arms. New York: Cambridge University Press, 1994. p. 259.
[5] Fuchida, Mitsuo and Masatake Okumiya. Midway: The Battle That Doomed Japan. Annapolis: Naval Institute Press, 1955. p.96.

enemy carrier task force appearing on its flank. The vague reply suggested no response plan existed. Nothing was done to prepare for such an eventuality. In fact, this was just the eventuality that occurred at Midway.

Third, the war games ended with many of the officers in the operational forces dissatisfied over various aspects of the plan, in particular the underestimation of enemy capabilities. Because they failed to voice such reservations, the plan marched on while planners failed to address the various problems and underlying assumptions.[6]

[6] *Ibid*., p.94-99.

APPENDIX 5. DRAFT MEMO FROM THE SECRETARY OF DEFENSE

A DoD culture that is more conducive to taking risks needs to be more attentive to understanding these risks. Red teams can be a major contributor, not only by "playing" the adversary, but also by challenging our assumptions, plans and programs. I look to red teaming as a disciplined way to deepen our understanding of options available to adversaries, to make our assumptions, plans and programs more robust and to avoid the complacency that often follows success.

I want more effective use of red teams in DoD. As a first step, I am creating several red teams to help identify the lessons that potential adversaries (nations and other) could be learning from recent US military campaigns. The USD (I), working with the USD (AT&L), USD (P) and the VCJCS will establish the teams and report back to me in 60 days.

In addition, to strengthen our use of red teams, I have directed:

- USD (AT&L) to develop, distribute and continually update, a best practices guide for red teaming
- CJCS, USD (AT&L) and the Service Chiefs to establish red teaming as a subject to be researched and taught at institutions of PME
- Department and Agency Heads to report back to me on their plans for enhancing the role of red teams in their own organizations

Red teams are not an oversight function. Embedding the use of red teams in DoD's culture will increase our understanding of the risks as we make major changes and transform our military capabilities.

APPENDIX 6. GLOSSARY

ACTD	Advanced Concept Technology Demonstration
AFB	Air Force Base
SAF/AQLR	Secretary of the Air Force / Acquisition Special Programs Red Team
AT&L	Acquisition Technology and Logistics
CEO	Chief Executive Officer
CHOP	Countermeasures Hands-On Program
CJCS	Chairman, Joint Chiefs of Staff
CMTC	Combat Maneuver Training Center
DART	Defense Adaptive Red Team
DCSINT	Deputy Chief of Staff for Intelligence
DLA	Defense Logistics Agency
DoD	Department of Defense
DSB	Defense Science Board
Intell	Intelligence
JFCOM	Joint Forces Command
JRTC	Joint Readiness Training Center
MC02	Millennium Challenge '02
MDA	Missile Defense Agency
MIT	Massachusetts Institute of Technology
NTC	National Training Center
OEF	Operation Enduring Freedom
OIF	Operation Iraqi Freedom

ONA	Operational Net Assessment
OPFOR	Opposing Force(s)
OSD	Office of the Secretary of Defense
P	Policy
PME	Professional Military Education
RDO	Rapid Decisive Operations
SAF	Secretary of the Airforce
SDI	Strategic Defense Initiative
SDIO	Strategic Defense Initiative Organization
SecDef	Secretary of Defense
SSBN	Subsurface Ballistic Nuclear
TF	Task Force
TRADOC	Training and Doctrine Command
TRANSCOM	Transportation Command
UK	United Kingdom
US	United States
USD	Office of the Under Secretary of Defense
UV01	Unified Vision ‘01