Playing the Bad Guy:
How Do Organizations Develop, Apply, and Measure Red Teams?

James Michael Fleming

Dissertation submitted to the faculty of the Virginia Polytechnic Institute and State University in partial fulfillment of the requirements for the degree of

Doctor of Philosophy
In
Public Administration/Public Affairs

Anne M. Khademian
Randall S. Murch
James F. Wolf
Thomas A. Hickok
Colleen A. Woodard
Matthew M. Dull

26 April 2010
Alexandria, VA

Keywords: alternative, analysis, adversary, defense, intelligence, war gaming, red team, red teaming, war fighting, terrorism

Playing the Bad Guy:
How Do Organizations Develop, Apply, and Measure Red Teams?

James Michael Fleming

Abstract

The study is a descriptive analysis using a case-study methodology that identifies the critical elements (methods, tools, processes, personnel, and practices) of adversary analysis identified as a *red team* and *red-teaming*. The study incorporates interview data with organization leadership, subject matter experts, and red-team developers from Department of Defense (DoD), Intelligence Community (IC), and Federally Funded Research and Development Centers (FFRDC) organizations. The study incorporates red-team governance artifacts and interviews to first identify the concepts, analyzes the critical design elements of the concept(s), and finally develops a taxonomy of red-team approaches. The study compares and contrasts four red team approaches for common themes, differences, and best practices. The data collection builds on grounded theory—i.e., identification of the methods, tools, processes, and personnel as the organizations understand and develop their red teams as part of their red-teaming analyses to address gaps in understanding possible adversaries. The four organizations studied are the U.S. Army, Training and Doctrine Command; a Department of Defense unified combatant command; the U.S. Naval War College (NWC) and its red-team detachment; and a Sandia National Laboratories (SNL) Homeland Security and Defense, National Infrastructure Simulation and Analysis Center (NISAC). Two basic types of red teams are identified from the data with a hybrid between the two types. Some of the other findings from the four red teams include a need to develop common terms and standards; a need to explain the benefits of alternative analysis to decision makers; a need to develop trend analyses on types of red teams requested by sponsors; a need to design methods to capture non-state actors; a need to include more coalition and foreign partners; and a need to immerse red teams more fully into the culture to be understood.

This dissertation is dedicated to my wife Alexandra, my daughter Natalie my son Garrett, my committee chair Anne Khademian, and my committee mojo Randall Murch

Table of Contents

List of Tables and Figures

(All tables and figures are created by the author unless otherwise cited)

Figures Page

Terms of Reference

Adversary analysis: The theoretical universe of approaches and frameworks that can analyze an adversary prior to engagement. Red-teaming and red teams represent one of the best-known branches of adversary analysis and provide an entry point into discussion of the process, including development, application, and measurement of the practice.

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. The study takes an expanded view and includes a diversity of activities that, while differing in some ways, share fundamental features. Red teams are established by an enterprise to challenge aspects of that very enterprise's plans, programs, and assumptions through a series of analytical tools, techniques, and procedures. It is this aspect of deliberate and systematic *challenge* that distinguishes red-teaming from other management tools, although the boundary is not a sharp one. (Many tools are used by management for a variety of related purposes: to promulgate visions, foster innovation, and 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.

Generally, a red-team challenges components of an organization 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 strategy, 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).

Red team: The red team is the mock aggressor. The methodology of red-teaming or acting as a pseudo-aggressor is the focus of this study. A red team can demonstrate potential harm a real attacker could inflict and expose weakness or gaps and risks to the processes, organizations, or technologies of the sponsoring organization (called the blue) team.

The analytic technique of war-gaming: A war game simulates or represents a military, government, or commercial operation. War-gaming is an analytic technique that utilizes this gaming approach in a multistep process that can also be called conflict simulation. The somewhat-similar professional study of war is generally known as a military exercise or "war game" (note that war-gamers have traditionally run the two words together, but the military generally has kept them separate). Although there are occasional disagreements about what qualifies as a war game, the general consensus is that they are not only games about organized violent conflict, campaign, or warfare, but that they must explore and illuminate or simulate some feature or aspect of human behavior directly bearing on the conduct of war.[1] Types of war-gaming include table-top exercises and computer-based or live (with actual forces playing blue and red) modeling and simulations (M&S).

Blue team: The blue team (or system) is the U.S. military, intelligence, leadership elements, law-enforcement organizational unit(s), or commercial sponsor of the game employed in the exercise or simulation to give the sponsoring agency the ability to identify vulnerabilities overlooked by system developers and defenders in lieu of a real attack. At the completion of the exercise, after findings and observations are reviewed, the blue team may be modified, improved, or trained differently.

Modeling and simulation (M&S): A physical, mathematical, or otherwise logical representation of a system, entity, phenomenon, or process. M&S covers a large subset

of war-gaming and provides the framework for testing new processes, organizational elements, and/or technologies in a controlled environment. When this new element is operated or engaged within a scenario, a series of findings and observations may be ascertained through modeling and simulating. The findings are then interpreted for relevance and validity and modifications may be made to the element.

Scenario: Possible alternative future event or condition that can be gamed by an exercise to produce analytic outcomes. Scenarios allow improved decisionmaking by stimulating more complete consideration of different outcomes and their implications. Scenario planning and analyses provide a framework for a group of analysts to generate simulation games for policymakers. The games combine known facts about the future, such as demographics, geography, military, political, industrial information, and mineral reserves, with plausible alternative social, technical, economic, environmental, educational, and political trends from which findings, outputs, and other key observations are derived.[2]

The scenario is the key to a tabletop or other war-game exercise. It must be definitive yet realistic in that it defines the mock conditions that will exist at the beginning of the exercise to:

- Test an approach or model;
- Explore new relationships, conditions, or gaps;
- Better understand intricacies that may exist in a system or environment.

A successful scenario can test hypotheses or standard operations related to threats or capabilities in a safe test environment before the real crisis or dramatic increase in operational tempo occurs. The scenario should provide the organization with a series of findings that allow the organization to improve its operations before finding out too late that new processes, personnel, or technologies do not work as expected.

Simulation*:* A method for implementing a model over time. A simulation can also be a series of techniques for testing, analysis, or training in which real-world systems are

used or where a model reproduces real-world and conceptual systems. M&S are often referred to in three different variants: live, virtual, and constructive.[3]

Types of simulations: Another method of categorizing government and military simulations is to divide them into two broad areas.

Heuristic simulations are run with the intention of stimulating research and problem solving; they are not necessarily expected to provide empirical solutions.

Stochastic simulations involve, at least to some extent, an element of chance.

Most military simulations fall somewhere in between these two definitions, although manual simulations lend themselves more to the heuristic approach and computerized simulations to the stochastic.[4]

Constructive* M&S*: M&S that contains elements of virtual and live (people and/or systems) is called constructive M&S. Usually constructive M&S is used when modeling weapons systems that would be too expensive to conduct completely with live firing exercises, and any outputs or findings would be too unrealistic to perform virtually as well.

***Live* M&S:** Field training exercises involving troops and actual equipment (i.e., real people operating real equipment). Live simulations allow soldiers to use organizational equipment under actual environmental conditions that simulate combat. The live simulation provides ground test data on actual hardware and software performance in an operational or development environment. In addition, the data can also be used to validate the M&S used in the acquisition program. Live simulations provide the stress and decisionmaking that is associated with human-in-the-loop simulations. In addition, the introduction of multiple types of platforms allows for evaluation of actual interaction and interoperability. *Test* modeling and simulation involves conducting data collection in an environment where variables are strictly controlled except the model or approach

undergoing the actual test. The testing framework still must support the model-test-model concept by calibrating M&S output.

***Virtual* M&S:** M&S conducted with the help of the Internet and communications technologies has fostered a decoupling of space where war-gaming events can seemingly happen as if real. These technologies allow simulations to be built and conducted virtually, by virtual work in teams, with members who may never meet each other in person. Communicating by telephone and e-mail, with work products shared electronically, virtual teams produce results without being co-located.

Tabletop exercise: The tabletop exercise is a popular and fairly uncomplicated method of testing war-game concepts, business/mission continuity plans, or other scenarios. This type of exercise provides valuable training to personnel and enables planners to enhance conceptual plans without causing major interference of normal operations. A tabletop exercise can be defined as "one method of exercising teams in which participants review and discuss the actions they would take per their plans, but do not perform any of these actions. The exercise can be conducted with a single team, or multiple teams, typically under the guidance of exercise facilitators."[5]

White team: No matter the type of exercise presented, facilitators or an exercise planning coordinator is crucial for successful execution. The white team selects the type of exercise to be performed and is responsible for selecting the components of the plan to be exercised. For a tabletop exercise, it's the responsibility of the coordinator to:[6]

- Identify the objectives;
- Develop an initial exercise scenario and narrative;
- Identify the participants and manage their collaboration;
- Chair and facilitate the exercise;
- Perform a post-exercise analysis;
- Develop a scoring method relative to the response of the participants as their plans are implemented during the exercise.

Chapter 1. Introduction

1.1 Overview

The multidisciplinary technique of modeling and simulation, known informally as "war-gaming," is an analytic exercise. It allows theories or practices of warfare or other government operational activities to be tested and refined against a mock adversary without the need for actual hostilities or expensive, resource-intense field exercises. This mock adversary approach is called a *red team*. The application of this red team to theories, practices, or operations via a war game or other testing, prototyping, or simulation is called *red-teaming*. War-game simulations exist in many different forms with varying degrees of realism. Recently, the scope of simulations has widened to include not only military but also political, intelligence, and social factors, which are seen as inextricably entwined in realistic warfare models. The red-teaming approach has seen a widespread increase in use and found new applications post-9/11.

While many government organizations make use of simulations using red teams, both individually and collaboratively, little is known about the practice outside of professional circles. While modeling and simulation can be conducted virtually using algorithms and computer-based calculations of dependent variables and behavior, some simulations lend themselves to using pseudo-adversaries pulled from a community of subject-matter experts, academe, or the ranks of operationally experienced active-duty personnel with expertise in the discipline to be simulated. These actors make up the red team to realistically portray the adversary in order to simulate his or her behavior and test and refine military and political governance, doctrine, mission processes, weapons and systems, organizational interfaces, or training.

While military simulations are a useful way to develop tactical, strategic, and doctrinal solutions in specified, controlled environments, they can be dependent on the accuracy or realism (or lack thereof) of the pseudo-adversary or red team. The organization's *team* or government forces or systems undergoing the test/refinement or improvement are called *blue* teams. Red team/blue team simulations and exercises take their name

from their military antecedents. The idea is simple: One group of expert professionals--a red team--attacks something, and an opposing group--the blue team--defends it.

In the 1990s, industry and government analysts began using red team/blue team exercises to test information security systems. Today, with Overseas Contingency Operations (OCO) in Afghanistan and Pakistan and Operation Iraqi Freedom (OIF), the complexity of non-state transnational threats, and tribal and religious elements, have been called into question many military and intelligence doctrines and operations. Despite massive investments of men and materiel, success and effectiveness in understanding and countering these new threats has been elusive. This dissertation examines red-teaming as a vital analytic tool in understanding adversaries by documenting how four organizations develop red teams—specifically the methods, tools, personnel and processes that organizations utilize to develop red teams. No study of this nature has previously documented red-teaming across these defense, intelligence, and civilian domains.

As American national security planners and war fighters have been caught off guard by terrorism, non state actors, urban and civil unrest, religious sects and factional violence so have their tactics and strategies. From the Tanzanian and Kenyan embassy bombings, the USS Cole bombing and 9/11; to the “Global War on Terrorism” and the effectiveness of Improvised Explosive Devices (IEDs) in Iraq on coalition forces, new adversaries’ and their evolving and adapting tactics have forced national decisionmakers and commanders in the field to reassess tactics, techniques and procedures, operations and strategies. Large uneducated peasant masses, urban populations, and small numbers of nebulous radical Islamic organizations led by mullahs steeped in 9^{th-} century doctrine and 21^{st-} century off-the-shelf technology continue to create much more of an impact than any other threat on American national security planning[7]. The United States’ national defense and intelligence communities are striving to understand the drivers of this new enemy including culture and thought processes—not only operational capabilities, weapons and modus operandi. Red teams appear to be a key analytical tool for supporting these efforts.

Yet, outside their specific operational environments, little is known about the ways in which red teams are developed, how they are used, what benefit they provide, and whether they are useful, even though they continue to be utilized. This study sheds light on the analytical concept of red-teaming. It compares different approaches to red-teaming by looking at four organizations that claim to do it; a U.S. Army training command "schoolhouse"; a nationally recognized war-gaming center; an operational combatant command; and a Government-owned, contractor-operated research center. It then compares and contrasts the tools, personnel and processes and products of the red teams for gaps, common themes, and best practices.

STUDY QUESTIONS

1) How do four organizations engage in red team development and use?

2) How do these four organizations validate red team methods, measure their effectiveness, and improve red-teaming?

The results of the study allow a more complete examination and understanding by academe and users of red-teaming methodologies developed and employed by these defense and national security organizations. Questions addressed during this study include: How does an organization go about creating this red team? Does a red team actually work to capture adversaries' way of thinking, planning and operating? Are agencies and military organizations using red-team outputs to change/improve operations? Is there an accepted definition of a red-team way ahead?

1.2 Scope of the Study

Red teams, although relatively unknown outside private sector information technology and defense and intelligence analytic communities, fill a very interesting analytic void that includes adversary behaviors, yet resource limitations, shortages of critically thinking designers, and the absence of defined and documented red-team design and

methodological standards limit the development and application of such an approach. The study captures red-team methods to support development of standards of what, how, and where red teams purport to, can, and systematically do enhance analysis, decisionmaking, and strategic planning.[7]

The data collection builds on grounded theory to first identify the methods, tools, processes, personnel, and practices the four organizations use to develop their red teams and then build a case for a typology in context with each. Red-team organization leaders and subject matter experts were interviewed and their published documentation collected and analyzed using grounded theory to identify the personnel, approaches, and processes for a red team and red-teaming compilation. The four organizations studied were the United States Army Training and Doctrine Command's (TRADOC) University of Foreign Military and Cultural Studies (UFMCS); a Department of Defense unified combatant command (COCOM); the United States Naval War College (NWC) Office of Naval Intelligence (ONI) red-teaming detachment; and Sandia National Laboratory (SNL) Homeland Security and Defense mission area-based National Infrastructure Simulation and Analysis Center (NISAC).

Each of the organizations' operational contribution to intelligence and defense, and mission differ substantially. Their operational problem sets range from tactical squad, platoon, and company operations to entire enterprise and strategic long-term policy-planning doctrine and asset protection. Their uses of red teams differ dramatically and with different contexts—however constants are identified and similarities and differences noted.

The outcome of this dissertation is the development of a standardized set of key characteristics and a framework that categorizes the different approaches to red-teaming within a context and provides the foundation for a *methodology* to develop more measurably effective red teams (i.e., one that captures and validates adversary behaviors, thought processes, approach to problem solving) for use by military and intelligence professional red-team developers across multiple domains. Because four

very different organizations were compared, there were a number of areas and topics that were outside the scope of the study and may be areas of further study. They include formal red-team training requirements, red-team accreditation, and the insertion of non state actors into threat emulation red teams.

1.3 Study Synopsis

The study compared different approaches to red-teaming by looking at four organizations that claim to do it; a U.S. Army training command "schoolhouse"; a nationally-recognized war-gaming center; an operational combatant command; and, a government-owned, contractor-operated research center. It then compared and contrasted the design, development, use, and outputs of the red teams for common themes and best practices.

Two major approaches were identified for using red teams. One is a traditional threat emulation approach that focuses on free-form play. Interaction occurs between red and blue teams with much qualitative, and some quantitative, criteria and outputs in the form of predictive evaluations; (NWC/ONI Det model is a primary example). These red teams are traditional in the sense they have a cadre of subject matter experts; access to specialized knowledge, skills or abilities which are tailored per event; and the support of organizational leadership to market the red-team capability and be referred to by outside organizations. These red teams are developed to "play" the role of adversary and seek to test a blue team in a one or two-sided game. A series of hypotheses, all relevant background information, a scenario or a situation may be provided by the sponsor, refined by the red-team staff, and the degree of latitude between teams is provided in advance based on parameters to see what transpires. The exercise is then run and data is collected to prove or disprove the original hypothesis.

The second major red-team approach focuses on recruiting, training, and equipping internal cadres of military, civilian, and intelligence professionals to think more broadly

(i.e., taking culture, economics, politics, and other social phenomena into the process) about operational and strategic problem sets. These professionals are then embedded into Combatant Command planning and integrated priority processes. These embedded red teams view operational challenges and problem sets from a different perspective to identify courses of action that may result in unintended consequences before they are implemented or recognize courses of action that may bring about desired responses from an adversary or neutral entity in that Command's area of responsibility. These red teams also may work to provide red analytical products or develop evaluation documents that analyze red decisionmaking processes and responses. This approach seeks to embed alternative analysis inside the very structured and somewhat rote traditions of government, military, or intelligence doctrine; (i.e., the UFMCS and DIOCC/JIOC models).

Red teams also exist that try to combine the characteristics of the aforementioned approaches and apply rigorous systematic methodologies. These might be labeled "hybrid" or combination red teams that tend to take on some characteristics of both threat emulation and decision support red teams. These teams may rely on very structured methods, tools, techniques, and procedures like the SNL-NISAC vulnerability assessment approaches. The red team is but one element that is mechanistically applied only at the threat definition and adversary sequence diagramming steps to fully understand threat courses of action and determine the steps necessary to neutralize it. This red-team approach may rely on simulations and exercises which focus on logarithmic equations to calculate factors such as risks, threat, vulnerability, and assesses their characteristics as part of a larger systematic evaluation that is more holistic in nature. The red team is an embedded factor that is transparent to the overall analysis. This analytical evaluation approach delivers predictions of system or system component performance within an overall system effectiveness framework. Further, it identifies exploitable weaknesses in asset protection, physical security, or cyber attack and is designed to support management decisions regarding system upgrades in the form of defense, security, or virtualizing system assets (SNL-NISAC model).

1.4 Contribution to the Literature

This dissertation examines the organizations' different red teams and their personnel, processes, and technologies and compares them for some contextual understanding of what exactly constitutes a red team. In current existence but in limited academic papers, there is information systems asset protection red-team literature, war-gaming red-team literature, and even a small amount of red-team literature in the information technology, asset protection, and military sciences disciplines; However, there is a gap in describing how U.S. agencies tasked with intelligence and defense responsibilities formally develop red-team adversaries and the process they use to simulate adversary behaviors especially to create, design, and validate red teams that are intended to simulate an adversary. There is little publically-available literature on formally defining, designing, developing, or operating a red team.

Nor is there a concise definition of what series of threats, capabilities, and plans result from use of such a team in an exercise or simulation scenario. Lastly no red-team experts or sponsoring organizations have documented standards by which to design, use, or measure red teams to establish or improve effectiveness and value. This is important as red-teaming in the context of a non-Western adversaries is expected to be a priority for military, intelligence, homeland security and perhaps law enforcement organizations in the West for the foreseeable future.

Some commercial entities such as consulting firms and large defense or federal systems integration contractors actually provide *tailored* analyses of red-teaming that is output based-not input or process focused. Private sector-conducted red-teaming results are held very closely by the government organization paying for the studies. Measures of red-team effectiveness understandably are strongly biased towards the agency paying for the study and influenced by the agency mission. Inherent bias in private sector studies, due to the desire to generate more business cannot be discounted. Little information is available despite the fact red-team outputs could support intelligence, save lives, and provide data points that can help predict the plans, tactics or strategies U.S. adversaries are likely to use and what their courses of action

they may take in some situations or scenarios[8]. The methods used by red teams are seldom shared in publically available literature for a number of obvious reasons including use by adversaries to adapt to new strategies that successfully target them.

This study addresses this gap and makes a contribution to literature by comparing, analyzing, and documenting red teams in four organizations in four different operational environments. Additionally the study examines each of the four organizations' red-team processes and related information (Depending on organization this can include development, governance, implementation, operations, and after-action reporting).

Chapter 2. Current Red-Team Models

Given the fact that red teams are not well documented outside their particular domains and results of red-team analytical products are the property of their sponsors, there is little formal literature on their formation. However, there are three particular domains that have at least repeatedly embraced the technique in various forms. The defense/military establishment, the information technology sector, and the homeland security/physical protection domain represented by federally funded research and development (FFRDC) labs such as Sandia National Laboratories have publically acknowledged an interest, use, and development of red teams.

For the purposes of this study, these three domains provide the best sources of existing red-team documentation including models, approaches, and guidance. Unfortunately, the artifacts organizations in these domains reference are a patchwork with little standardization, sharing of best practices, or academic rigor. Additionally, the definition *red team* can mean a host of practices, analysis, adversary concepts, and threat definitions which support a wide variety of analytical objectives within the domains.

Given current events and the possibilities red teams provide, red teams may appear to be some sort of analytic panacea if they can just incorporate the “right” recipe of sociological, paramilitary, and asymmetric warfare expertise. However, each of the domains to be explored in this section approach red teams differently.

Non-technical and sociology-focused red teams generally come from sources other than the domain conducting the red team. This expertise may indeed come from academia, non-profit institutions and non-governmental organizations, the military (including former military), intelligence (including former) and diplomatic (including former) communities. In leveraging these different agencies, academe, or other subject matter experts may give the red team some substantive or perceived realism in comparison to an adversary of the blue team, however, there is no quality or performance standards that ensure red-

team builders have captured whatever dynamicism or non-linear perspective of the new or exotic adversary that is desired.

As emphasized earlier, there are no standards or industry guidelines that certify when a red team is sufficiently "real" to validate its findings. There is no agreed-to certification process that allows red-team analytical results or findings to ensure the right skills are being sharpened, the correct vulnerabilities were strengthened, or the right assets were protected—without exposing new weaknesses, losing needed skills, or forgetting about assets that were ignored in the red-team study.

2.1 DoD/Military Rational Decisionmaking Approach

The military services, especially the Army and Navy, long have used elements of the red-teaming process, particularly war games to think through campaigns. The Army defines *war game* as follows: "A disciplined process, with rules and steps that attempts to visualize the flow of a battle. The process considers friendly dispositions, strengths, and weaknesses; enemy assets and probable courses of action; and characteristics of the area of operations."[9] The war game may be a disciplined process with rules, but red-teaming has fewer rules and steps unless there are mechanisms to ensure its realism and its disciplined application versus the blue team.

Additionally, the Air Force Doctrine Center's *Aerospace Commander's Handbook for the JFACC [joint force air component commander]* mentions the notion of war game red-teaming, although it provides no further details. Some elements of red-teaming are as basic and intuitive as a pilot simulating a mission before execution. Malone and Schaupp emphasize the need for peer review and vulnerability assessment applied to the combat air patrol process at several levels.[10]

Red teams used in military war-gaming tend to be threat-based and can be costly to assemble and require much more lead time for complex planning and staging. However, their benefits can be much more far reaching. The discovery of the utility of aircraft

carriers during the 1930s Pacific Fleet war games helped defeat the Japanese in the Pacific. Due to budget limitations, infrequency, and the use of static scenarios that can influence red-team findings, often their size and utility is questioned by Congress and proponents of other readiness effectiveness measures. However, the Committee on the Iraq Study Group and the current Joint Chief Of Staff Admiral Michael Mullen strongly believe their use can avoid mission failure and possible catastrophe.[11]

The Defense Science Board (DSB) chaired by Schneider (2003) identified four domains where red teams can and do play an important role within the Department of Defense (DoD). These include:

- Training
- Concept development and experimentation (not just an opposing force [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 test (for example, nuclear weapons stockpile issues)[12]

This list is not exhaustive and as the reader will discover, red teams can and are being utilized across the government agency spectrum to solve a variety of problems from civilian agency cyber-warfare vulnerability to U.S. military combatant command decisionmaking rigor.

The DoD/Military model often includes a diversity of activities that, while differing in some ways, share fundamental features that comprise an adversary perspective designed in some manner to oppose a blue team in a controlled test or proto-typical environment prior to the blue force, doctrine, concept going live or operational. It is this aspect of deliberate challenge that distinguishes red-teaming from other DoD 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, etc.)[13]

Malone and Schaupp (2004) of the U.S. Air Force, define red teams as an approach that studies, simulates, and role-plays the enemy and outside agencies during Air Force crisis action planning (CAP) exercises that can go far toward providing a non standard perspective to role play against. In this context, they offer the following working design definition of red team: a group of subject-matter experts (SME), with various, appropriate air and space disciplinary backgrounds, that provides an independent peer review of products and processes, acts as a devil's advocate, and knowledgeably role-plays the enemy and outside agencies, using an iterative, interactive process during operations planning.[14] This approach is steeped in the rational decisionmaking model because it involves a cognitive process where each step follows in a logical order from the one before. By cognitive, it is based on thinking through and weighing up the alternatives to come up with the best potential result[15] (see Figures 2-1 and 2-2).

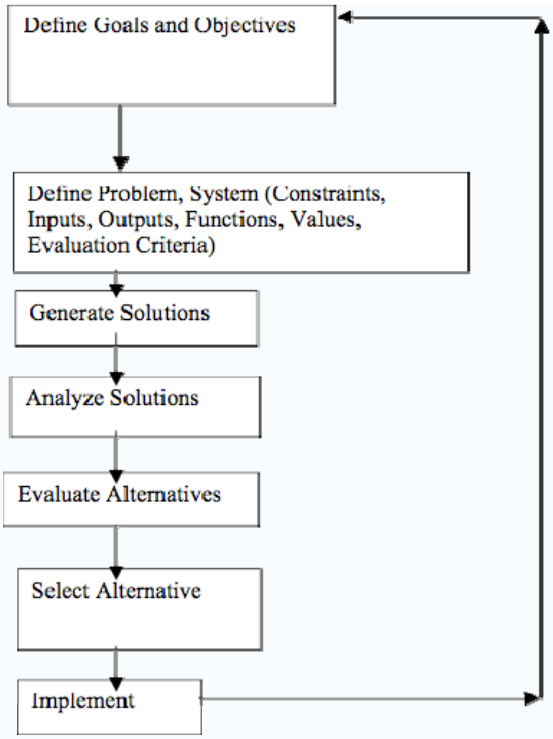


Figure 2-1: Bounded Rationality Model

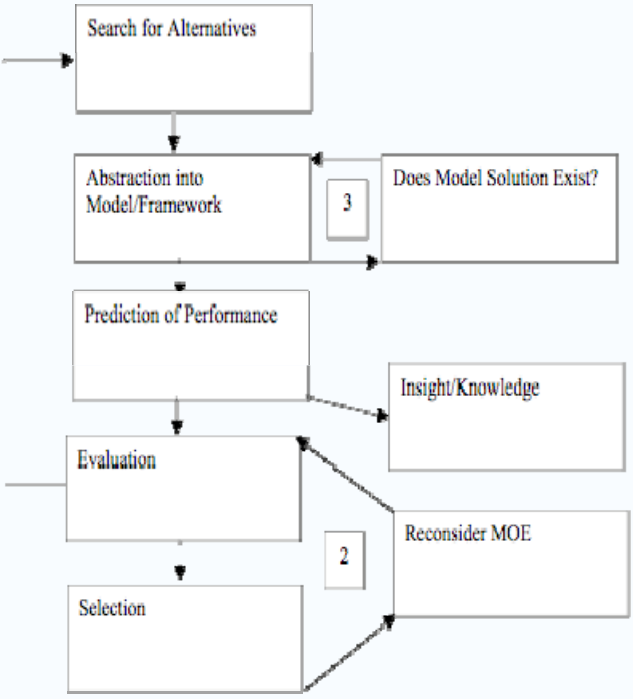


Figure 2-2: DoD/Military Red-Team Model[16]

There are different types of rational models and the number of steps involved, and even the steps themselves, will differ in different organizations depending on the blue team system or attribute to be tested.

As the reader can see from the DoD/Military Red-Team Model, it is based on a rational approach model that takes problem set or goals, possible solutions, alternatives, and evaluates those alternatives based on knowledge, data, and predicted performance. To ensure that independent knowledge is applied, Malone and Schaupp (2002 and 2004) discuss red-team composition from an Air Force perspective and believe the (red-team organizer) commander should draw red-team members from sources external to the blue planning organization.[17] Although this may seem intuitive, it is not always easy to accomplish.

Most organizations that have the necessary experts are usually fully employed- indeed, the Blue planning organization itself is a perfect example. A commander may be tempted to utilize his or her own blue planners as the red-team members; after all, what better people to assess a plan than the ones most intimately familiar with it? But this seemingly workable solution can be flawed because one of the prime benefits of red - teaming is an independent review of blue operations and reasoning.[18] Even the most talented planning group often cannot discern its own oversights (Malone and Schaupp, 2002, 2004). As concerned as blue team planners must inevitably be with the details, it is sometimes difficult for them to stand back and see the larger environment.[19]

Malone and Schaupp strongly suggest red teams for tactical operations and crisis action planning applications but the Defense Science Board (2002) red-team findings advised red teams to be developed to address a much wider problem set:[20] Whereas Malone and Schaupp were looking at red teams for improving courses of action for air warfare, the DSB looked at red teams as a component of a structured test environment for new technical as well as doctrinal, training, and strategic approaches. The DSB reviewed current DoD red-teaming activities and developed a series of findings based on

interviews, independent assessments, and after-action reviews. They include the following points of current successful DoD red-team activities:

> 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 some DoD outsiders 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[21]

Once the red-team experts are identified, their focus turns to preparation. The team discusses and anticipates the red-blue engagement in an iterative, interactive series of events that closely parallels the military service or agency processes.[22] Therefore, red team members have to immerse themselves in learning everything they can about what has gone before in the event to be studied at hand and what the enemy and other adversaries are thinking. Joint Publication (Pub) 5-00.2, Joint Task Force Planning Guidance and Procedures, provide a list of actions that planners must accomplish to prepare for war-gaming during COA analysis.[23] These DoD joint publications tend to emphasize the *what* rather than the *how* and this may be a rather large flaw in the approach. But without introspection and comparison between red teams, it is not known.

Since the scope of red-teaming can be significantly broader than that of war-gaming, the Air Force red team prepares its own preparatory checklist, based on the joint publication’s guidance (Table 2-1 below). Neither exhaustive nor necessarily applicable at every step, the checklist nevertheless has proved useful because it provides some

disciplined approach to the application of a red team against the blue team in Air Force war-gaming events. [24]

Malone and Schaupp's Red-Team Checklist
Red-Team Preparations Checklist
• Establish secure location away from distractions
• Access to Secret Internet Protocol Router Network (SIPRNET), Joint Deployable Intelligence Support System (JDISS), and Unclassified but Sensitive Internet Protocol Router Network (NIPRNET)
• Maps and overlays
• Office supplies
• Gather necessary reading material and data
• Chairman of the Joint Chiefs of Staff (CJCS) warning order and directives
• Combatant commander warning order
• Other major command or higher headquarters guidance
• Relevant message traffic (intelligence reports, etc.)
• Combatant commander's assessment
• Relevant briefings or documents produced to date in the planning process
• Relevant publications (joint pubs, planning guides, etc.)
• C2 diagrams or task-organization information
• Blue COAs under consideration
• Country studies
• Enemy order of battle
Prepare to role-play the enemy and other adversaries
• Review country studies
• Study enemy doctrine and force disposition
• Identify C2 infrastructure and decision-making processes
• Identify enemy centers of gravity (COG)
• Identify Blue COGs as seen by enemy
• Identify enemy's limiting factors (LIMFAC)
• Identify enemy commander's key decision points
• Determine enemy's anticipated COAs
• Study the political environment
Understand the overall situation and Blue planning progress
• Review assessments, orders, messages, and other products
• Identify and assess Blue assumptions
• Identify Blue LIMFACs
• Identify known, critical events in the operation
• Identify Blue commander's key decision points
• Convene a Red Team meeting to review elements of the crisis

Table 2-1: Red-Team Preparations Checklist[25]

Red-team sponsors naturally have biases and predilection towards results that validate their planning or operational approaches; for example, most U.S. Navy red teams seldom included non state actors or the employment of naval craft smaller than gunboats prior to the USS Cole bombing (for which zodiac boats were used). The U.S. Air Force red franchise (above discussion) training is not designed to use civilian aircraft as an air attack method. U.S. ground forces entering Iraq in 2003 did not secure extremely potent stockpiles of 155 millimeter artillery rounds (the primary explosive component of IEDs). If the simulation is intelligence community-focused, the red-team exercise may lack technological or military realism; if the exercise is war college-generated, it may not contain the religious or cultural nuances necessary for a valid finding. Any combination of these compromises can limit the lessons learned from the red-team exercise. Even more dangerous, it may lead to type II errors (i.e., the blue-team technology, doctrine, training, approach is falsely assumed to be *sound*).

Traditionally, religion or culture has not been as significant as technology, or weapon systems in military environment. Additionally, the operational dangers of groupthink and blind acceptance of Western war fighting principles and assumptions are well-documented. These are such perceptions as: *control of the air equates to control of the war; strategic bombing breaks their will to resist; one enemy center of gravity always exists; tribes can always be bribed; and some finite amount of resources can replace village safety concerns do exist currently among deployed battalion commanders*. Those who challenge these and other accepted principals and assumptions do so at their own peril.

General Billy Mitchell was ostracized by the “Battleship Admirals” who found his idea that battleships were vulnerable from the air personally offensive during the interwar period. Nevertheless, organizational senior leadership and defined rules of engagement are critical to successful red-team exercises—inside and outside DoD to conduct what C.C. Palmer (2001) characterizes as "no-holds-barred" activities against the specified systems or processes.[26] In a control audit engagement and a red-team penetration test,

the best results may come from testing systems that are in normal and routine operations as the next red-team model in Section 2-2 shows.

There are many elements within the Air Force that believe red-teaming, if conducted effectively, can yield a closely synchronized planning staff, drive more complete analysis at all phases, and ultimately deliver a better plan of operations into the hands of a war-fighting commander. Within the Air Force, senior officers have realized an effective red teams can pinpoint key *blue* decision points, identify planning shortfalls, show deviations from doctrine, reveal overlooked opportunities, and extrapolate unanticipated strategic implications.[27] Just as important, good red-teaming, according to Air Force doctrine, determines how clearly *Blue* planners understand the tasks that higher headquarters have given them and indicate whether they must request additional, specific guidance for planning critical facets of the operation.[28]

Military/DoD red-team construct champions such as Malone and Schaupp and the DSB reinforce the application of the red-team decisionmaking model is a rational approach to maximizing the blue team's choice of alternatives. The model allows the blue team to select the goals, build the process, implement, and evaluate courses of action from alternatives. Two case studies examine this DoD/military bounded rational model in Section 5.

As red teams tend to be comprised of individuals selected for their special subject matter expertise, perspective (professional, cultural), imagination or penchant for critical analysis, there is no standard that ensures the process all works according to plan. 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.[29] For example, the Undersecretary for Defense (Intelligence) (USD(I)) has set aside resources for each Unified Combatant Command to maintain internal red teams within their joint intelligence operations centers (J-2) to test planning theories and assumptions before implementation. This type of red team is one of the four case studies in the study. Two other case studies

are also DoD approaches, one being a traditional threat emulation red team and the other a newer type of red team based on OIF war fighting lessons learned from the U.S. Army that challenges many past cultural and technical assumptions and is a promising new model for use across the DoD.

2.2 Commercial Information Technology Industry Model

Red teams and red-teaming processes have been used in various capacities as tools by the private sector management of both government and commercial enterprises. Their purpose is to reduce an enterprise's risks and vulnerabilities and increase its opportunities by applying an adversary against the enterprise (blue team) in a controlled environment. Red teams come in many varieties (virtual and SME) and there are different views about what constitutes a red team. This study takes an expanded view from an intelligence and defense communities' perspective sanctioned by the Defense Science Board on what exactly constitutes a red team. However, in the commercial world, red teams are established by an enterprise to challenge aspects of that very enterprise's plans, programs, assumptions, etc.[30] which generally focuses attention on commercial information systems' vulnerability.

The commercial red team often must strike a careful balance with management even more so than the DoD model. On one hand, to gather the most accurate results, it may be necessary for management to accept that critical systems may malfunction or data may be lost during the red-team testing; on the other, the red team must not push the systems beyond the agreed-upon parameters or there could be a loss of equipment and profitability.[31]

Many organizations' utilize red teams or what some in the information technology (IT) industry call "white-hat" hackers. The use of these teams is primarily during a security assessment or audit that incorporates a red team to determine how vulnerable a system is or how an adversary could compromise a system to steal or destroy information. A

whole information assurance (IA) industry has sprouted during the last decade to combat this danger. According to Gallegos (2006), an IA red team or *white hat hackers*, is composed of individuals skilled in performing ethical hacking—employing the same tactics malicious hackers may use against information systems, but instead of damaging systems or stealing information, the findings are reported back to the organization. Information Systems (IS) auditors can use the red-team method to their advantage to gain a better understanding of new and emerging security threats and produce actionable proof to make the case for fundamental changes in an organization's IA security practices.[32]

Similar to Malone and Schaupp (2002), Gallegos (2008) states that red teams made up of internal staff are problematic. If they are internal, they already have knowledge of the network and security. This violates the rule of "testing" one's own systems. Therefore, auditors who are hired from outside the company to conduct a red-team audit are not given prior information about the network or security to simulate a true exercise in external intrusion. Thus, they can provide an external, unbiased test of the control infrastructure. The recent Carnegie Mellon report on insider threats points to the fact that external threats and internal threats need separate approaches.[33]

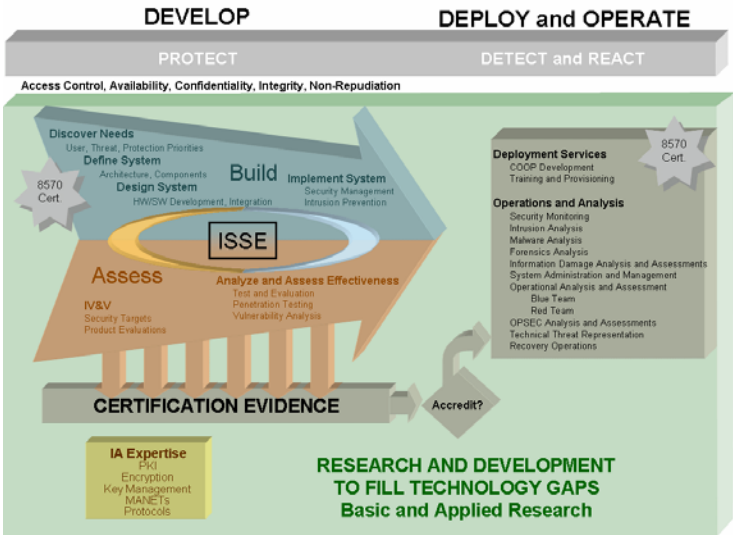
According to Gallegos (2006), firms navigate around these and other obstacles that may roadblock a successful red-team engagement by ensuring red-team auditors have the acceptance from management that the judgment of the red team is valid and tolerate criticism of established corporate practices.[34] Gallegos argues that the red team must have not only top management support but also a comprehensive agreement with the organization undergoing the application of the red team that outlines the evaluation plan and identifies the exact systems or processes to be examined prior to the exercise. Without an explicit, written assurance guaranteeing that the team is free from liability, there is a significant risk that the team may be subject to penalties (in the civilian sector this could include criminal), as it could be possible, for example, for the team during their testing to unintentionally intrude on systems that may be governed by the laws of other countries, accidentally violate the integrity of systems connected to the

organization via an electronic trading system, or view highly sensitive, patented or secret material.[35]

The successful corporate red team is composed of competent subject matter experts (SMEs) with experience appropriate to the engagement.[36] For information technology red teams, according to Gallegos (2006), both the participating auditors and red team technical specialists have, at a minimum, a firm grasp of the fundamentals of computer forensics and a good general knowledge of the systems and processes against which they will test.[37] The red team typically tests four areas of an information system:

- Information residence, or operating system platform and storage security
- Information transmission, or networks and communications
- Information use, or the applications and decision processes based on data generated or collected by the information system
- Information access, or the policies, passwords and permissions used to gain access to data[38]

Figure (2-3) below depicts a notional commercial red-team approach based on systems engineering principles and IA blue-team objectives. Analyze and assess or risk



Figures 2-3: Example of Commercial IT Industry Red-Team Approach[39]/[40]

analysis is often the step whereby the red team tests the system vulnerability prior to implementation in the best cases. Other commercial IT red team approaches include Van Der Walt's (2002) seven steps in the security lifecycle where red-teaming can be inserted as part of any of the steps.[41] However, software engineering institutes and educational and certification-granting organizations strongly advocate implementing security practices which may include red-team applications prior to achieving operational status. Many capability maturity model integration (CMMI) and the IT International Organization for standardization (ISO) 9000 standards advocate rigorous security testing of systems.

More IT-focused red teams provide independent assessments of information, communication and critical infrastructure to identify vulnerabilities, improve system design and help decisionmakers increase system security, their processes are tied to the information security life cycle above.[42] The red-team process is more tightly bound to systems engineering domain as it is an assessment function in a larger program management system. That it can yield valuable information that can be used to form a clear, objective picture of an organization's information security practices and identify vulnerabilities is an added benefit. Red-teaming practices can also be used later in the life cycle by information security and auditing professionals to retest systems and procedures to determine if the suggested changes were successful and implemented.[43]

According to Gallegos (2006), with thousands of known IT vulnerabilities and tens of thousands yet to be discovered in a given system, the red team must be careful to avoid scope creep by attempting to test for the irrelevant or trivial during the attack planning stage. The attack tree is one innovative method that can help define and manage the scope in both types of engagements. Figures (6-7 to 6-10) in Section 6 provide examples of attack trees.[44]

In a red-team attack tree, the overarching goal of the attack, for example, cracking into an organization's database, is represented at the top of the tree as the root node. To crack into the payroll database, a sub-goal, which is represented by a sub-node of the root node, might be to guess the password to the database or to copy the database in

its entirety.[45] Each of these goals may have sub-elements, or highly specific, tasks that can be done to accomplish it, such as "run a database password cracking tool." These tasks will take the form of leaf nodes in the attack tree. After the attack tree has fully taken shape, the red team can evaluate each leaf node using capability analysis. In capability analysis, the team will make an estimation of the cost, ability and tolerance of apprehension of the attack.

Therefore, in an attack tree illustrating cracking into the payroll database for example, it may be determined that the cost of using a freely available password cracker tool is US $0, the ability level is very low, and the tolerance of dishonesty, or likelihood that someone would use this method to crack the database without the fear of getting caught, is minimal.[46] On the other hand, the risk of copying the database, which may be on a standalone computer, may be quite high if the attacker has to resort to stealth and physical intrusion to get to the computer. As the red team evaluates each possibility and weighs the chance that an attack is likely, the least likely options are pruned from the attack tree.[47]

As commercial red teams are less tradition-bound than military red teams and may have more culturally diverse red teams, they are still tied to the systems engineering domain. Despite relatively more cultural awareness, they may or often do not have the flexibility or charter from senior management to look at non-IT threats such as cutting power, vandalism, terrorism, or flood damage. In summary, military/DoD red-team models have come from threat emulation roots and commercial red-team approaches have come from the IT discipline. Both have strengths and weaknesses that have been recognized by critics. One organization that has attempted to bridge the divide is Sandia National Laboratories (SNL). SNL has created a number of red team and threat assessment frameworks that *quantifies* military rule of thumb guesswork or experience and system engineering and other threats into algorithmic equations based on impact or likelihood. Because of this red-teaming expertise, this study has selected Sandia National Laboratories' federally funded National Infrastructure Simulation and Analysis Center (NISAC) as the commercial case study.

2.3 Sandia National Laboratories (SNL) IORTA/IDART Methodologies

SNL has recognized red teams can do more than play the opposing force (OPFOR) as in threat emulation applications; some red teams provide independent assessments of information, communication and critical infrastructure to identify vulnerabilities, improve system design and help decisionmakers increase system security. According to Seltzer (2007), Sandia National Laboratories *Information Operations Red Team and Assessments*™ (IORTA™) Program red teams provide independent, objective assessments of information, communication, and critical infrastructure systems throughout their lifecycles (concept through retirement) in order to identify vulnerabilities, threats, improve design, and assist decisionmakers with choices in development, security and use of their systems. The program focuses on malevolent intent of adversaries and applies a wide spectrum of methodologies, tools, research, and training to achieve organizational security goals.[48]

Unlike Malone and Schaupp's OPFOR model, Sandia's IORTA and Information Design Assurance Red Team (IDART™) has been performing assessments since 1996 for a variety of customers including government, military, and commercial industry. Through its participation in a variety of government programs and leadership of industry conferences, the IDART team has assembled one of the best known and standardized theory and practice of red-teaming in the nation.[49]

IDART, part of the Information Systems Analysis Center at Sandia National Laboratories, continues to perform assessments to help its customers acquire an independent, objective view of their weaknesses from a range of adversaries' perspectives. At the same time, IDART, drawing on nearly sixty years of Sandia experience in assessment, is committed to evolving the practice of red-teaming and training qualified organizations, even helping such organizations stand up their own red teams.[50]

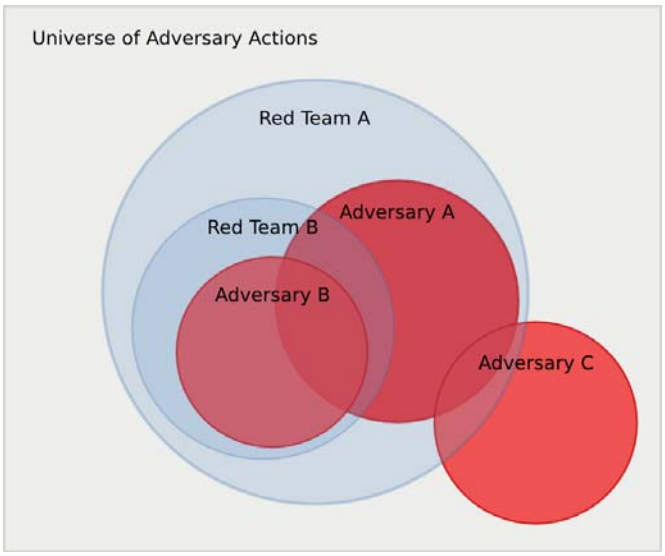


Figure 2-4: Venn Diagram of Adversary Actions[51]
(Used with permission of S. Holinka, Sandia National Laboratories, 2010)

The Information Design Assurance Red Team apply their craft principally to cyber systems, however, red-teaming is appropriate for use in multiple domains: physical security, control systems, chemical/biological/radiological/nuclear/explosive (CBRNE), defense, corporate strategy, etc. (Physical Security is the focus of the fourth case study in Section 6 because it is the most similar to the red-team subject matter of this study). The IDART red-team processes utilize adversarial modeling to enhance its assessment process and provide better completeness and consistency. In IORTA, this modeling can be described as a script of motivations, goals, and intent an adversary may hold for various environments. Such modeling helps to identify vulnerabilities that will be exploited, predict behavior in a scenario, and identify intent in forensic data.[52] Figure (2-4) above illustrates the entire universe of adversary actions and shows how red teams may be made up of numbers of different adversaries thereby allowing collaboration and feeding off each others possible actions.

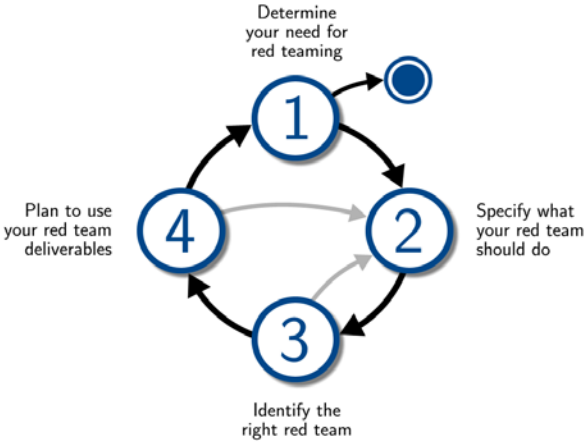


Figure 2-5: Four Step SNL IDART Methodology Components[53]
(Used with permission of S. Holinka, Sandia National Laboratories, 2010)

Figure (2-5) above illustrates an overly simple IDART red-team process insertion method that seems to suggest any time is good for a red team. Similar to Malone and Schaupp's red-team model which leverages the same information available to the blue team but with different red-team "players", Seltzer (2007) states that Sandia's IORTA process performs assessments of infrastructure (i.e., information systems, information flow, and decisionmaking which can include decisions on system, organization, company, and U.S. Critical Infrastructure systems) from the "red" or adversary perspective. The red team of this IORTA approach is called the *Information Design Assurance Red Team* (IDART) which provides the independent assessments of critical information systems that are:

- Performed from an adversary point-of-view
- Consequence-based
- System oriented

Seltzer (2006) infers the usefulness of IDART design methodologies because they can be used against blue-team information systems and in a variety of mission contexts including, networked computer-based systems, wireless systems, and process control systems. [54] Figure (2-6) below was taken from the Sandia National Laboratories IDART

website (2010) and depicts the iterative nature of the methodology which collects, characterizes, and analyzes multiple possible adversary engagements with the system to develop algorithmic equations based on a number of threat paradigms. These are more fully explained in the fourth case study in Section 6.

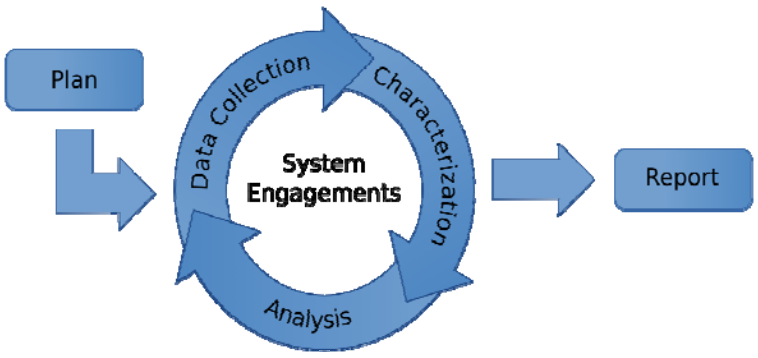


Figure 2-6: IDART Process Flow[55]
(Used with permission of S. Holinka, Sandia National Laboratories, 2010)

For the Sandia IDART model, the decision to pursue or forego red-team testing should be predicated on the results of an extensive risk assessment beforehand. In any risk assessment, the audit team should attempt to use best practices for risk assessment to categorize risks by severity. If there are severe or undefined risks present for the organization's critical, high-value systems or projects, red-team testing may be easier to justify than if the systems are noncritical and of low value.[56] A sample threat profile is shown below in Figure (2-7). A Sandia National Laboratories red-team methodology called the Vulnerability Assessment is discussed in Section 6 as the fourth case study in this paper.

THREAT LEVEL	THREAT PROFILE						
	COMMITMENT			RESOURCES			
					KNOWLEDGE		
	INTENSITY	STEALTH	TIME	TECHNICAL PERSONNEL	CYBER	KINETIC	ACCESS
1	H	H	Years to Decades	Hundreds	H	H	H
2	H	H	Years to Decades	Tens of Tens	M	H	M
3	H	H	Months to Years	Tens of Tens	H	M	M
4	M	H	Weeks to Months	Tens	H	M	M
5	H	M	Weeks to Months	Tens	M	M	M
6	M	M	Weeks to Months	Ones	M	M	L
7	M	M	Months to Years	Tens	L	L	L
8	L	L	Days to Weeks	Ones	L	L	L

Figure 2-7: IDART Threat Profile Table

(Used with permission of S. Holinka, Sandia National Laboratories, 2010)

2.4 Summary of Red-Team Operational Environments

Cordray (2007) has documented red-team practices in the Defense Intelligence Agency and that list is discussed at length in Sections 5 and 6. McGannon (2007) believes that red-team documentation should be available to all to enhance the discipline.[57] Governments, industries and public institutions appear able to benefit from a red-team approach to assessing threats to their facilities, personnel and supply chains. To avert surprise attacks, all potential targets must learn to see themselves through the eyes of the threat. There are two red-team methods used by international consultancies and academe—operational red-teaming and analytical red- teaming.[58]

Depending on war game scenario or goal, operational military red teams are focusing more on the decisionmaking of government agency planners, combatant command staff directorates, international and regional decisionmakers, military or joint task force commanders, and in-country government intra-agency teams.[59] The objective of operational red teams are centered more on definition of the interaction between agencies, elements, and components and not so much a technical fix or technological vulnerability. Additionally, Paller, (2005) states that when red teams within agencies find a blue-team vulnerability, they write up a report about it—and the system developers quickly fix the problem without documenting or adding it to an accessible

knowledge base. An actual thinking attacker will probe for multiple vulnerabilities and adapt to *fixes,*[60] an agency that didn't find the weakness will continue to operate with it.

In summary, the red-team analytical environment is very dynamic and contains many threads back to other disciplines and domains such as systems engineering and the military sciences that appear to leverage the approach. The horror of 9/11 combined with the difficulty in Operation Iraqi Freedom and Operation Enduring Freedom have funneled additional resources to the DoD to improve decisionmaking and analytical rigor. However white hat hackers, fashionable methods, and latest trends garner attention, the analytic approach suffers from multiple interpretations, models that do not transfer outside their sub domains, and questionable analytic rigor. It is difficult to identify and much less understand standardized methods, performance metrics, and types of red teams.

There is so much variance between red teams even within domain models. The lack of analytic standards appears to have resulted in anyone calling their assembled adversary experts a "red team." Nevertheless, in the post 9/11 environment, military, commercial, and think tanks are embracing the approach as a way red teams are ultimately intended which is to identify blue vulnerabilities. The real problem is without standards, there is no accountability when the red team has not identified all blue weaknesses and the blue system is fielded or deployed and catastrophe results.

Despite the DSB study and others advocating against it, members of the sponsor or blue team usually are selected as members of the red team in the military/DoD rational model. This appears to be due to significant barriers to entry such as culture, systems complexity and security constraints. Additionally, Herbert Simon (1957, 1976) identified rational approaches to human choices (i.e., decisionmaking) as being bounded by cognitive limitations such as imperfect information, time constraints, and access to all alternatives and all their consequences.[61] The forward deployed commander in the field has these constraints as does the battlefield. If red-team standards and training are

developed to recognize, address, and assess the correction of these limitations then the commander's decisions and the unit's effectiveness can be improved.

The Commercial IT red-team model is based on simulating malicious hackers who want to steal or destroy information for nefarious purposes. It is generally conducted virtually, somewhat rote, and outside the purview of this study because it is based more on having adequate reactive system protection approaches in place such as information security architectures such as firewalls, demilitarized file space, and network enclaves. Additionally, antivirus software protection tends to be in a binary competition with hackers who are trying to outsmart its code to allow penetration of malicious software to access vital information. There is a red-teaming aspect to what strategies and tactics may be employed as defensive approaches, but explanation would require much more emphasis on systems engineering simulations and information technology disciplines and is outside the scope of this study of human interactive red-teaming.

The Sandia National Laboratories model takes a systems approach that borders on the learning organization approach as articulated by Senge (1994 and 2005) discussed the concept of systems thinking, i.e., that organizations are a system of interrelationships and to become more successful in learning and adapting, we need to analyze these relationships and eliminate obstacles to learning and improving.[62] SNL's approach is to assist organizations in transforming themselves into more efficient, safer, better protected, less vulnerable positions vis a vis their position before a red team. The SNL approach is also a defensive vulnerability-focused red team but is robust enough to capture a wider spectrum of threats from engineering software to thinking attackers. Because the SNL red-team approach can capture both systems engineering and social science disciplines in a formally documented methodology, it was selected to be one of the case studies. The vulnerability of SNL's approach is that it does not have a method to deal with the fact or assumption that many organizations are fragmented, competitive, and reactive in nature. These types of qualitative aspects are not easily factored into quantitative models yet can derail very well thought-out plans.

Chapter 3. Red-Team Literature Review

3.1 Introduction

Mateski (2004) has tried to define an overarching red-teaming taxonomy and found none exists. No one has attempted to link disparate fields using a common grammar, definitions and relationships.[63] The Services, Combatant Commands, other governmental organizations, military academies' battle labs, joint modeling and simulation centers, commercial IT industries, other governmental organizations, and FFRDCs each define the concept and develop approaches differently.

This section addresses the basic three models articulated in Section 2, and identifies the gaps in the red-team literature. As Mateski has correctly articulated, there is no coherent taxonomy or categorical placement of red teams into subgroups to distinguish threat emulation red teams from decision support red teams. As the reader will see, the literature lacks the rigor, context, and standardization to distinguish red teams by even the blue-team problems they are attempting to address.

3.2 DoD/Military Red-Team Literature

As noted previously, the Department of Defense (DoD) has been a leading proponent of red-teaming exercises and thus a leading organizational contributor to red-teaming literature. Given the practitioner perspective of such endeavors, general findings and heuristic assessments tend to be in report form for the sponsoring agency. Few government, and even less DoD sponsors, want results or exact methodologies published for security reasons. Nevertheless, red-team contributions to the record include a number of entries according to the Defense Science Board Task Force on the role and status of DoD red-teaming activities (2003).

The DSB (2003) has at least agreed that red-teaming is a needed analytic tool and it is especially important now for the DoD. Current adversaries are very different 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.[64] The DSB (2003) believes 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.[65] The red team itself is only one element in a red-teaming process. The process can be explicit or ad hoc. Red-teaming as a process is as varied as the many organizations that conduct them. Elements of the process may 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. The DSB (2003) identified three types of red teams which include 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).[66]

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" (OPFOR in military parlance), using the adversary's presumed tactics and equipage (actual or virtual). Examples include the Army's OPFOR, the Air Force's at Nellis AFB, the Navy's OPFOR at Fallon and Key West, and *white hat hackers* in cyber red teams.[67]

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 U.S. 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 U.S. 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 Submarine Ballistic Nuclear (SSBN) Security Program[68] discussed in the literature review section.

Devil's advocates: 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 a process or how an organization conducts its business. An example of such a team was the Ballistic Missile Threat Committee that Secretary of Defense 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.[69] Examples include the U.S. government's Red Cell and the Joint Chiefs of Staff Chairman's Action Group (CAG) stood up by ADM Michael Mullen.

General Advisory Boards and other sources of independent judgment: The objective is often to be a sounding board and "kitchen cabinet" for the sponsor.[70] Examples include presidential panels that look into disasters or crises; Intelligence Community "graybeard" studies chaired by retired agency directors; and Congressionally-appointed panels convened to study and report on public sector systemic failures.

Although the Department of Defense has used the concept of red teams since the 1920s, their effectiveness has been blunted by the inability to establish standards and metrics for their use outside or across domains where they are originally developed. Red teams are commonly used at the tactical level to simulate opposing forces at the services' war colleges and battle labs. Since 9/11, many organizations within DoD, have been receiving additional funding for red-teaming efforts but have not established governance mechanisms to ensure the funding is well spent[71]

The U.S. Navy's SSBN (Submarine, Ballistic Missile, Nuclear) Security Program provided one published red-team program.[72] Established in the 1970s, the program identified potential vulnerabilities that the Soviet Union might exploit to put U.S. SSBNs at risk. The program also had a "shadow" (silent) customer in the Navy's own antisubmarine warfare programs. The focus of the program shifted in the mid 1980s to evaluate and assess findings from the intelligence community. Recent work has involved SSBN protection vulnerabilities, terrorist threats, and port security.[73] Schneider (2003) acknowledges the SSBN Security Program assesses threats and vulnerabilities based on a stated hypothesis relating to physical principles and operational realities and thus represents one form of red-teaming.

These assessments tend to be determined by technological feasibility and operational realities, not noticeably different or better than information system red-teaming that takes a set number of threats and mathematically determines which threat is most likely, and then puts in place a security system. But there is little discussion of an innovative calculating adversary who may not play by the physical principles or operational realities laid out in the security hypothesis. For example, port security should take on a whole new meaning after the USS Cole bombing but there is no discussion in the literature of that ever happening. It is unclear from the literature whether the SSBM red-team model is looking at physical protection system assessments in light of new threats as outlined by the attack on the USS Cole. A physical protection system red-team approach is the fourth red team discussed in this study in Section 5.

Though the scope and focus of the SSBN Security Program has changed over the decades, its guiding principles have remained largely unchanged.[74] Although adversaries have not yet shown the sophistication to attack SSBN bases or boats, the SSBN Security Program assesses threats and vulnerabilities based on decades old physical principles. These assessments are determined by technological feasibility and operational realities, not on new thinking or possible unconventional warfare using non-traditional methods.[75]

The U.S. Army's Red Franchise organization was established in 1999 within its Training and Doctrine Command (TRADOC) (Schneider, 2003).[76] The Red Franchise organization guides Army training, concept and force development, experimentation, and transformation. Red Franchise is responsible for defining the *operational environment* for any next two decades. This is codified in Army and joint publications 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."[77] This *operational environment* is the intellectual foundation for transforming the Army from a *threat-based* force to a *capabilities-based* objective force.[78]

The Red Franchise has a great deal of latitude from TRADOC customers and interagency communities (defined in this instance as other Army and joint elements such as the Combatant Commands and military intelligence organizations). The Red Franchise has also developed products such as the Joint Operational Environment and the Opposing Forces (OPFOR) "instruction manual" at the Joint National Training Center (JNTC).[79] According to Schneider, this instruction manual provides guidance on the composition and behavior of opposing forces.[80] Red Franchise also makes heavy use of outside experts but Schneider is not clear on where these experts originate or what key contribution the Red Franchise approach provides outside doctrine development.

The Red Franchise and the new Army Center for Lessons Learned appear to have given TRADOC the momentum to continually challenge the thinking of Army

commanders. It is still unclear as to whether the battlefield or the Red Franchise is more responsible for improvements and this lack of clarity was rectified in the first case study which focused on TRADOC in Section 5.

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.[81] MDA has 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 at all with the blue team. These red teams develop suites of penetration aids that an adversary might design to respond to blue missile defense systems. There is no counter move or interaction with blue designers to develop countermeasures or test red outputs an adversary might design and deploy in response to a U.S. 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.[82] Thus they are missing the key component of behavior and behavior modification in response to blue-team stimuli.

The MDA red teams were typically as interested in blue assumptions about the threat as in actual blue capability. This form of red-teaming requires a continuous and detailed exchange of information between the red and blue teams.[83] It is the Office of the Secretary of Defense's (OSD's) impression that in spite of good intentions, this type of red-teaming has been difficult to achieve and sustain in the MDA program due to a number of factors (Schneider 2003). The primary factor is the difficulty in fostering significant interchange between red and blue teams. This lack of blue-team interaction is somewhat common, however it may limit the robustness of the red team and render findings less useful in an era of evolving and dynamic adversaries.

The U.S. Air Force's literature on the subject has attempted to initiate a documentation process for developing successful red teams. They offer the following as a practical definition of the red-teaming process: "An iterative, interactive process conducted to assess planning decisions, assumptions, courses of action (COAs), processes, and products from the perspective of friendly, enemy, and outside organizations."[84]

The Air Force Red Team Program is located in the U.S. Air Force Directorate of Electronics and Special Programs (SAF/AQLR). According to Schneider, the red team provides assessments of concepts and technology (as opposed as serving as 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. SAF/AQLR's process involves making judgments (in part based on open literature) about the knowledge used and capabilities of future adversaries. These red teams may involve the intelligence community in the process to get additional classified input and collaborate with other black efforts.[85] This type of adversary-centric red-teaming is closer to the study topic but many of the SAF/AQLR findings focus on design and testing of Air Force technology programs, engineering studies, and doctrine.[86]

Their process involves red/blue interaction in order to evaluate and recommend blue system improvements. They argue their approach: [87]

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

A measure of this 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 SAF/AQLR program focuses primarily on system design and testing which makes it very similar to the commercial IT

red teams which are focused on structured system security algorithms and not necessarily on dynamic and non-linear threats.

According to Schneider, the OSD's Defense Adaptive Red Team (DART) Activity was established by the 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 combatant commands such as the United States Joint Forces Command (USJFCOM), 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 war games and experiments; conducting vulnerability/failure analysis for concepts; doing development of alternative or competing concepts (known as "Team B"); providing an independent assessment of experiments; identifying best red-teaming practices; and providing a framework for concept development and evaluation for the joint staff.[88] *Team B* is an OSD euphemism for alternative approaches, however DART is primarily focused on technology. According to the Defense Science Board (2003), USJFCOM has been using red teams for joint concept development and experimentation. Due to this information, this study was originally planning to use the USJFCOM red-teaming approach as a case study. However, upon contacting the combatant command, JFCOM Joint Intelligence senior personnel stated that JFCOM does not develop their own red teams but uses defense intelligence SMEs from other sources.

Nevertheless, the Defense Science Board states that 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 the Defense Science Board 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. Command representatives 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.[89]

Understanding the difference between an experiment and an exercise is important. Concepts can fail; experiments fail only if nothing is learned.

Ad hoc red teams tend to be developed and staffed by resourceful experts or retired government officers who have little vested interest in existing doctrine or intellectual dogma and nothing to gain politically. They may wish to demonstrate shortcomings via mock application of a theory or practice before real humans are killed much like "tough love". The red-team commander utilized small fast attack craft to defeat a massive 16 ship blue force carrier battle group in a 2002 Millennium Challenge exercise that embarrassed the Navy and validated blue force vulnerabilities to Iranian and Chinese fast attack craft. The unexpected tactics and results were strongly discounted by the Navy and defense contractors who build the ships and weapons systems of the defeated ships.[90]

JFCOM's red-teams also validate joint concept development and experimentation Rickerman (2003) and Darken and Sullivan (2002) discuss JFCOM's, use of red-teams for joint concept development and provide a number of little known outside the community examples. Some of these examples include *Rapid Decisive* and *Effects-Based Operations* and experimentation exercises like *Unified Vision '01*, *Millennium Challenge '02*, and *Unified Quest '03*).[91] From the literature, JFCOM has attempted to get red teams involved earlier in the concept development and experiment design process before large amounts of funds and personnel are committed. Rickerman, Schneider, and others have identified the difficulty in simulating new concepts in complex dynamic environments by focusing on experimentation and isolating failure or criticism before new approaches become new concepts and take on allies and detractors.[92] Little exists in the way of red-team assessment or determinants of success which is sponsored by JFCOM.

Darken and Sullivan (2002) also found that the challenge of using red teams effectively in experiments was highlighted by concerns expressed by the Opposing Force (OPFOR) [*red team*] commander in Millennium Challenge '02. Millennium Challenge '02 was billed as an experiment that would allow the OPFOR a measure of free play.[93]

The commander took advantage of this latitude and beat a far superior blue team using innovative tactics that were later deemed somewhat controversial (documentation of when and why red-team play was constrained after the blue team started to lose and the lessons learned/follow up analysis is classified). Instead, Millennium Challenge '02 was more a demonstration than experiment, involving an orchestration of events that ensured the blue team won and precluded key free play. This interference with possible valuable key findings was not documented so it is unavailable within the red-team literature.

The challenge of using red teams effectively in experiments was highlighted by concerns expressed by the person that played the OPFOR commander in Millennium Challenge II (MC02). MC02 was billed as an experiment that would allow the OPFOR a measure of free play however, MC02 was more demonstration than experiment, involving an orchestration of events that precluded free play. USJFCOM does participate in assessments of red teams which is why it was one of the candidate red-team organizations for a case study. However, it was not selected because the command does not design, develop or apply interactive red teams that respond to blue-team actions and vice versa.

Instructors and students at U.S. military war colleges have written extensively about adversary theory including war-gaming. Malone and Schaupp (2002) provided a general practitioner perspective with their paper on the U.S. Air Force's approach to tactical red-teaming and lessons learned. Malone and Schaupp note the concept of red- teaming is far from new. It has been used (under that name and others) in government, military, and civilian circles in a variety of contexts.[94] Malone and Schaupp emphasize the focus on enemy leadership decisions and reactions to the Blue campaign, the team included two opposing forces (OPFOR) experts and one specialist in integrated air defense systems, all from the intelligence career field. When possible, Malone and Schaupp advise red-team developers to recruit red-teamers from sources external to the blue planning organization. Although this may seem intuitive, it is not always easy to accomplish.

Most organizations that have the necessary experts are not available. Indeed, the blue planning organization itself is a perfect example. A commander may be tempted to use his or her own blue planners as red-team members. This may seem like a method to save resources and get the subject matter expertise that created the plan to assess the plan. Addressing the critical operational red-team practices and improvement touches upon what this study addresses. However, Malone and Schaupp barely touch the designing and building of a successful red team beyond what knowledge domains might be helpful.

In an article describing a notional "Silver Flag" red-teaming construct, Col Bobby Wilkes identifies an important red-team development initiative: "Develop a cadre of experts equipped with appropriate resources- *in-house red-team expertise*" (emphasis in original).[8] Because a red team will conduct a comprehensive review of blue planning products and processes, the selection of team members is critical. A commander should gather his or her red team from *functional aerospace disciplines that apply to the operation in question*.[95] Wilkes (2001) mentions Gen Gregory S. Martin, commander of United States Air Forces in Europe (COMUSAFE), tasked his command's first Red Team to assess an offensive air and space campaign. After analyzing requirements and considering the restrictions imposed by the "need to know," the Red-Team leader formed the team with SMEs from the following areas:

- Air operations and strategy
- Command and control (C^2)
- Joint operations
- Logistics
- Space operations and strategy
- Intelligence, surveillance, and reconnaissance (ISR)
- Combat search and rescue
- Information operations and information warfare
- Law
- Politics [96]

This formal listing is a start of properly documenting the multi-disciplinary needs of a red-team development effort but does not identify how such red teams can be developed, operated, evaluated or transferred to other disciplines outside the Air Force. Malone and Schaupp focus primarily on aircrew training, technology, and weapons systems.[97]

In summary of the available DoD red-team literature, the focus is almost always on challenges of development and implementation of red teams and the key elements a red team should provide in a resource and leadership rich environment. Additionally, the Malone and Schaupp and Silver Flag red-teams assume adequate knowledge exists if a red team is in place to collect it. In actual operations, there may be inadequate information or expertise available to the decisionmaker, time constraints, and resource limitations. If the red team does not have access to combinations of these vital elements, their value to the decisionmaker will be minimal or lead to type II errors. Literature on the DoD/Military red-team frameworks can be impressive but if they are not used, discounted, or ignored as they were recently in overseas contingency operations such as Operation Iraqi Freedom and Afghanistan, then their usefulness is suspect. Another recurring gap in the literature is little mention of a need for red-team standards or governance across domains.

3.3 Commercial and Private Sector Red-Team Literature

Red-team presentations and white papers from private sector sources and web discussions do not directly address the gap this study addresses because they focus on listing components of efforts vice a discussion of the full spectrum of design, processes, application, outputs, and success factors. Section 2 provided some IT-related red-team design, processes, and applications which form the bulk of the papers on private sector red-teaming. Section 6 deals more in depth with these issues directly by looking at Sandia National Laboratories National Infrastructure Simulation and Analysis Center (NISAC) and their approach in the last case study.

The little commercial literature available tends to come from trade publications and web-based IT system security associations touting the benefits of red-teaming. The literature can be divided into institutional studies that prescribe red teams as part of larger system or concept-development processes that test a security system, or the literature focuses on the benefits of unleashing information technology “white-hat” analytical hacking before the actual malicious hackers find your vulnerabilities for you. The former employ red-teaming practices and theoretical perspectives that are more ad hoc and used by information system detractors to highlight shortcomings in technical or strategic approaches. The latter employ red teams to assist in the conduct of effectiveness and prescriptive studies and analyses. These tend to be focused on fixing tactical shortcomings in a blue system. The latter use institutional red teams which incorporate their use into design and development processes of complex technical systems or multiple government agencies comprised of a series of information assurance processes that require vulnerability assessments prior to an implementation phase.

As discussed, commercial red-team literature is extremely weak and focused around the trade of products that allow good data through systems and stop malicious software and viruses. Gallegos (2006) states that red-team results should have immediate consideration and be acted a relatively short time period. At the team engagement, the final report organization should document all the steps and used in the course of testing. These must be detailed to satisfy concerns that sponsors might have about the introduction of new programs or loss of data caused by the team must have a documented plan. They clearly state specific steps that manage the risks identified during the initial possible recommendations found in a red to suggest to the sponsor or customer: [98]

- Apply a software update
- Change a firewall's access list to prevent intrusion
- Implement account and process auditing software
- Create and promote security awareness within the organization

If the red-team engagement was driven by a requirement to comply with legislation, auditors should attempt to answer the by offering specific and concrete steps to fulfill this need. For example, if the healthcare facility that had to comply with Insurance Portability and Accountability Act (HIPAA), the report should suggest steps the organization should take to comply with the HIPAA security mandate. This mandate requires that patient data and transactions containing patient data be safeguarded to protect confidentiality, integrity and availability, but does not give any suggestions or recommendations for how a provider can accomplish these goals. Auditors can reconcile the risks to patient data and the red-team's vulnerability assessment by using outside resources such as the American Medical Association's (AMA's) best practices publication, Field Guide to HIPAA Implementation, networking with other auditors and teams specializing in the same area, or drawing from past experience. A possible suggestion for this scenario might be to implement an encrypted virtual private network between two doctors' offices to deter hackers from intercepting transmissions of patient data.[99]

According to Gallegos (2006), the results of the red-team engagement must be kept discreet. Prior to the engagement, the organization should conduct a thorough background check of red-team members. Some complex systems may require third-party companies or freelance experts to help assist auditors in conducting the testing. It is important to make sure that these individuals are trustworthy beyond doubt due to the sensitive nature of ethical hacking. Finally, confidentiality agreements should be drafted by the organization and signed by the members of the red team prior to or after the engagement affirming that no information will be shared.[100] (in this instance, the recommendations are coming from a legal perspective—in order to be in compliance with the law.) In other instances, where the recommendations are coming from is not clear.

In summary, nearly all commercial sector red-team literature has an underlying goal and that is to “sell” red team or white hat hacker methods to other companies or government organizations that have large IT architectures and holdings. Even the trade

associations and other seemingly impartial red-team electronic and hard copy publications, are full of articles touting the benefits of letting experts hack into your information systems to identify vulnerabilities and develop mitigation strategies before the adversary does.

Chapter 4. Method of Study/Research Methodology

4.1 Fundamental Approach

A grounded theoretical case study approach was used to collect the red-team organizational leaders' objectives and subject matter expert (SME) data on each organization's approach to red-team development. The emphasis of the data collection was on personnel, frameworks, and processes used for red-teaming; i.e., describing the processes each organization engages in to ensure key red-team design parameters are met to ensure their definition of success; and the types and characteristics of personnel used for red-team design. Interviews with organizational elites and their red-team SME definitions of critical design frameworks, attributes, or approaches are captured. These attributes were evaluated for similarity, differences, and best practices so that grounded theory could be applied to develop a series of frameworks to achieve definition of and possible optimal red-team methodologies. Grounded theory was selected as the secondary approach because as data is collected, the conceptual understanding of red-team development and application evolves through continual interplay between analysis and data collection to identify similarities and differences in developing a framework.

4.2 Theoretical Grounding/Theoretical Frameworks

The purpose of this chapter is to give an overview of the methodologies to be applied to the study and the data collection approach. Corbin and Strauss 1990; Glaser 1978; Glaser and Strauss 1967; Strauss 1987; Strauss and Corbin 1990 have addressed grounded theory procedures and logic. Grounded theory is a general methodology for developing theory that is grounded in data systematically gathered and analyzed. Theory evolves during actual research and through continual interplay between analysis and data collection. This theory evolutionary approach is well-suited for studies that seek to define taxonomies and hypotheses where none currently exist.

A central feature of this analytic approach is “a general method of [constant] comparative analysis” (Glaser and Strauss, 1967); hence the approach is often referred to as the constant comparative method. Grounded theory methodology explicitly involves generating theory and doing social research [as] two parts of the same process (Glaser 1978). This “real-time” linkage of theory to research is still relatively unique but becoming more mainstream as are other new sciences such as Chaos Theory, Complexity Theory, and other post-modern theories become more accepted.

Because grounded theory is a general methodology, a way of thinking about and conceptualizing data, it was easily adapted by its originators and their students to studies of diverse phenomena. To name only a few, these included professional socialization (Broadhead, 1983), policy arenas (Wiener 1981), remarriage after divorce (Cauhape 1983), interaction between builders and a would-be homeowner (Glaser 1972), homecoming (Hall 1992), the management of a hazardous pregnancy (Corbin 1992), ovarian egg donation between sisters (Lessor 1993), spousal abuse (Lempert 1992), experiences with chronic illness (Charmaz 1980), and the development of general theory about status passages (Glaser and Strauss 1970).

Regardless of level of theory, there is built into this theory the extensive interrelated data collection and theoretical analyses, an explicit mandate to strive towards verification of its resulting hypotheses, and flexibility. This is done throughout the course of a research project, rather than assuming that verification is possible only through follow-up quantitative research.

The conceptualization of the red-teaming frameworks by the case study organizations for this study was developed from a key underlying interpretive sociological framework; i.e., social reality is meaningfully constructed and ordered from the point of view of the actors (Berger and Luckman 1967; Burrell and Morgan 1979; Weick 1979; and Pfeffer 1981). This framework allowed the researcher to focus on organizational processes, data, and personnel to determine how the red-team developers (1) frame the hypothesis; (2) design the exercise/simulation scenario; (3) execute the activities; (4)

derive findings and key observations; and (5) formally document lessons learned and define success or failure. In addition, as patterns of action become repeated, shared and social definitions of Red-teaming occur, i.e., emergent and situationally-defined action affects and is affected by culture, historical patterns and expectations and value systems[101] of the administrative participants (Clay 1989).

Since the primary method to be applied to the data is grounded theory methodology, it is advantageous to understand the approach and its limitations. Corbin and Strauss 1990; Glaser 1978; Glaser and Strauss 1967; Strauss 1987; Strauss and Corbin 1990 have addressed the methodology's procedures and logic. Grounded theory is a general methodology for developing theory that is grounded in data systematically gathered and analyzed. Theory evolves during actual research and through continual interplay between analysis and data collection.[102] This theory evolutionary approach is well-suited for studies that seek to define taxonomies and hypotheses where none currently exist.

The dissertation methodology researched red-team development based on four case studies leveraging the theory generation process in order to understand: (1) What hypotheses or questions are being asked that cannot be answered from other analytical approaches; (2) How scenarios and their red teams are designed and developed-- what mechanisms are in place to ensure realism and validity in terms of mimicking pseudo non Western adversaries' decisionmakers; and (3) How or are the resulting red-team scenarios executed? (4) How are key observations and other findings collected and is there a special process for including unintended findings or conclusions? (5) What is the process for documenting performance results and lessons learned?

To understand these five questions, the research methodology had to collect and address the data from red-team developers or SMEs.

4.3 Study Design

This research study identified four organizations that design, use and apply, derive outputs from, and improve analytical tools called red teams. The study then collected data on each red-team approach and analyzed the data to compare and contract each organizations approach. Finally the study categorized red teams into typologies.

A notional red-team development process (Figure 4-1) below shows the general steps necessary to design, develop, and implement, and execute a simulation or exercise. As a critical element of the effort, the concept of an adversary must be part of some initial hypothesis and then depending on scenario, have key characteristics that drive the development of some type of conceptual red-team adversary at step two; applies this red team against the blue team; and then evaluates some results towards the end of the process.

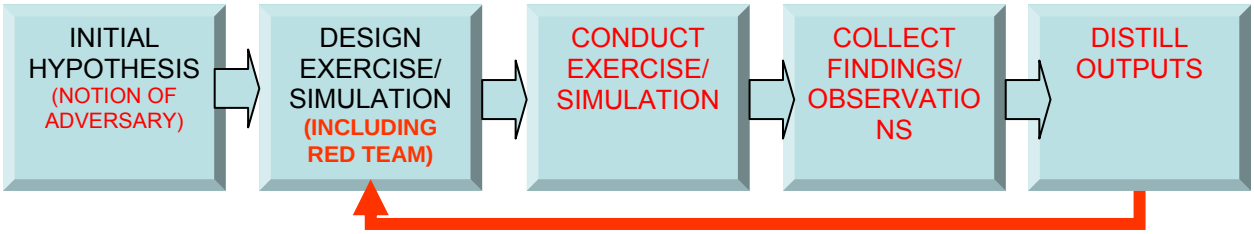


Figure 4-1:Notional War Game/Simulation Process (with Red Team Target of Study in RED)

In the case of this dissertation, the quintessential question is: "What is the process American intelligence and defense planners utilize to develop red-team adversaries for example, its theory, thought, practices, planning, doctrine, approach to management/scarce resources, ability to modify plans based on failure/success; into their red teams (where relevant) to act out possible adversary scenarios?" Stated differently, how do red teams incorporate non-Western culture and other attributes that do not necessarily include what Westerners would label attributes from Western eyes.

4.4 Data Collection

The data collection portion of the study utilizes a matrix format to collect information on each red-team sub process by utilizing the questions below. The initial framework for the study consists of a series of tables to capture each organizations red-team attributes. Once these attributes are documented, they are then compared to the other organizations throughout the study for impact on blue-team behavior and at the end of the study for overall impact, realism to actual culture, incorporation of religious themes, etc.[103]

This data collection process was implicitly utilized for this study with information and data intelligence community and Department of Defense red-teaming activities being gathered from:

- Unclassified official government reports and documents (e.g. investigation board reports, congressional committee hearing testimony, red-team guidance documents)
- Red-team print media artifacts (e.g. journals, books, periodicals)
- Interviews with war-gaming principals and elites from industry and government who have first-hand red-team knowledge and understanding

The ancillary analysis of the data attempted to fully develop a taxonomy or continuum model of unclassified red-team development approaches. This model was depicted in bipolar and quadrant figures in the last chapter of the document based on the data derived.

The survey instrument is based on the sample questions below:

1) What is the name of defense/intelligence organization and what customers does it support? Provide a background and experience summary or war games, blue and red teams.

2) Does the respondent have familiarity with concept of *red-teaming?*

3) What is the conceptual understanding of the organization in terms of a systematic approach to red teams?

4) Have there been recent war-gaming instances whereby the respondent had familiarity/interaction with key non-Western doctrine? Or have cells/groups who regularly consulted/participated when respondent was a participant and determine how such red–team participants gained "familiarity" or expertise and how this expertise is judged (quality, type, value)?

5) Did after-action report or game summary/findings reference or comment on cell/group robustness/adequacy in capturing realism of non-Western or non-linear behaviors?

6) Define successes.

7) Define failures or describe what could have worked better.

8) Provide any other data/points-of-contact for more detailed study.

What critical red-team development success factors are necessary to ensure capture of non-Western adversary attributes?

9) How should greater community maintain non-Western or non-linear adversary attributes such as networked or virtual organizations, Eastern concepts of time and space, saving face, concept of fate?

Note that follow-up questions to elicit information not provided or not satisfactorily provided through these questions will also be asked.

4.5 Data Sources

A number of organizations were contacted and their red-team activities were reviewed for candidacy in the study. The U.S. Marine Corps University, Training and Education Command's Center for Advanced Operational Cultural Learning in Quantico, Va.; National Defense University at Fort McNair in Washington, D.C.; U.S. Joint Forces Command in Norfolk, Va.; the U.S. Army Training and Doctrine Command's University of Foreign and Military and Cultural Studies in Ft. Leavenworth, Kan.; two Department of Defense unified combatant commands—one assigned to a geographic area of responsibility (AOR) and one assigned to worldwide functional responsibilities not bounded by geographic responsibilities; the U.S. Naval War College in Newport, R.I.;

and Sandia National Laboratories in Albuquerque, N.M. The organizations that were eventually selected are described below.

4.5.1 U.S. Army Training and Doctrine Command's University of Foreign and Military and Cultural Studies

U.S. Army Training and Doctrine Command (TRADOC) established the University of Foreign Military and Cultural Studies (UFMCS) at Fort Leavenworth, Kan., to provide the educational and training foundation to support the fielding of an Army-wide red-team capability. The curriculum is designed to enable red teams to support decisionmaking during planning and operations. Red teams identify potential weaknesses, vulnerabilities and unseen opportunities. Red teams also anticipate and account for the perceptions of partners, adversaries and others in our planning, and conduct independent and unbiased critical reviews and analysis of such items as concepts and experiments.

TRADOCs red teams provide commanders with an independent capability to explore alternatives in plans, operations, concepts, organizations, and capabilities in the context of the operational environment. They do this from the perspectives of Army partners, adversaries, and others. Red-teaming is a function executed by trained and educated officers, senior warrant officers, senior non-commissioned officers, and civilians to enhance staff planning and improve decisionmaking in today's dynamic and uncertain environment.

The organization was chosen because UFMCS supports the Army and TRADOC by institutionalizing the concept of red-teaming by adding red teams to existing force structure, adding the concept to doctrine, refining techniques and procedures, and continuing formal UFMCS conducted education and training programs at Fort Leavenworth and at unit locations.[104]

The Army is engaged in irregular and counter-insurgency operations or warfare "among the people" and has realized it must adapt its thinking to recognize and understand new dynamics of the global security environment. To effectively operate in these unfamiliar circumstances, the Army has begun a number of new initiatives that educates and trains its decisionmakers on the complex interaction among populations, technology, governments, military forces, and external factors as well as the cultures and the physical environment these complex interactions are underpinned upon. Initiatives such as "Every Soldier is a Sensor" (ES2), cultural awareness/language training, human terrain teams (HTT), mobile training teams (MTT), and red-teaming are imperatives and key to adapting traditional military processes and thinking to the current and future complex operating environments.[105]

The University of Foreign Military and Cultural Studies at Fort Leavenworth runs three high-quality "*Red Team*" training courses to develop critical thinking and nontraditional analytical skills aimed at identifying dependencies, unintended effects, vulnerabilities, and mitigating strategies. Red teams are expected to aid staffs during planning and operations by identifying potential weaknesses, vulnerabilities, and unseen opportunities. These teams will anticipate and account for the cultural perceptions of adversaries and others actors, and conduct independent and unbiased critical reviews and analyses.[106]

4.5.2 DoD Unified Combatant Command X

A unified combatant command (UCC), is a DoD command with a broad continuing mission under a single commander and composed of significant components of two or more military departments or services (e.g., Army, Navy, Air Force, Marine Corps). The president establishes and designates unified commands through the secretary of defense with the advice and assistance of the chairman of the Joint Chiefs of Staff.[107] This command structure of the DoD is defined by the Goldwater-Nichols Act of 1986. Under the act, the chain of command runs from the president of the United States, through the secretary of defense, to the regional commanders within one of several

commands who command all military forces within their area of operation. The specific command is designated as an *X* because the command has an area of responsibility (AOR) which would suggest red-teaming may directed at specific countries in the AOR.

All UCCs are also known as "COCOMs," or "combatant commands." They are led by combatant commanders (CCDRs), formerly known as regional "commanders-in-chief" (CINCs; pronounced "sink").

The organization was chosen because there are 10 Unified Combatant Commands. Six have regional responsibilities, and four have functional responsibilities.

COCOMs with Regional Responsibilities:

United States Africa Command - USAFRICOM (note: AFRICOM reached initial operational capability 01 October 2007, with full operational capacity slated for 01 October 2008)
United States Central Command - USCENTCOM
United States European Command - USEUCOM
United States Pacific Command - USPACOM
United States Northern Command - USNORTHCOM
United States Southern Command - USSOUTHCOM

COCOMs with Functional Responsibilities:

United States Joint Forces Command - USJFCOM
United States Special Operations Command - USSOCOM
United States Strategic Command - USSTRATCOM
United States Transportation Command - USTRANSCOM

4.5.3 United States Navy Naval War College Center for Naval Warfare Studies, War-gaming Department

The Naval War College's Center for Naval Warfare Studies is central to the Navy's research efforts in maritime strategic thinking. One of its departments, *War-gaming*, introduced at Newport in 1887, allows students, joint and fleet commanders, and representatives of the Department of Defense and various governmental agencies to test operational simulations and advanced strategic concepts more than 50 times a

year. Utilizing technologies such as video teleconferencing, computer simulation and web capabilities, the now named *Decision Support Center* offers users a selection of information gathering tools to support critical outcomes. Responding to the need to examine maritime strategy, the Naval War College is collaborating with sponsors to develop an extensive scenario analysis and war-gaming effort and a series of high-level conferences, symposia, and other professional exchanges with maritime partners around the world.[108]

War games, part of the Naval War College Gaming curriculum since 1887, are vehicles for generating, testing, and debating strategic and operational concepts, and for exercising military and civilian decisionmakers in maritime and joint warfare. War games do not prove or disprove theories, concepts, or strategies because they are not reality and cannot be duplicated. Nevertheless, war-gaming is an effective technique for creating a decision-making environment that fosters education and understanding for students and operational staffs, provides insights, and generates issues for further study. Groups of games set in the same theater or exploring the same or similar issues can help players to understand the dynamics of war fighting and may suggest possible trends or tendencies which could be exploited in real-world situations.[109]

The Decision Support Center War-gaming Department is a well-known gaming organization, conducting games and scenarios annually in support of internal College needs and externally generated requests from various branches of the Defense and Navy departments, operational commands and civilian agencies, including the Office of the Vice President of the United States, the Joint Chiefs of Staff, and the Secretary of the Navy. To support the objectives of each game's sponsor, the War-gaming Department employs a wide variety of gaming techniques including red-team design, development, and implementation. The games range from complex, multi-sided, computer-assisted programs to simpler, single-sided seminar games, and game foci can range from broad national strategies to the specifics of tactics. Most games take place at the College, but some are conducted off site.[110]

The Naval War College's missions are to develop strategic and operational leaders, help the Chief of Naval Operations define the future Navy, strengthen maritime security cooperation, and support combat readiness.

The organization was chosen because the college has two key elements that engage in red-teaming and red-team development. The Decision Support Center (DSC) provides an innovative environment for decisionmaking. The Office of Naval Intelligence (ONI) NWC Detachment provides the DSC with essential red-team capabilities which fall into four categories:[111]

- Analytic methodologies, decision support and warfare analysis tools that allow groups to brainstorm, evaluate, and prioritize critical problems and weigh alternative courses of action;
- High-tech communications that bring information systems, databases, and expertise together to solve critical problems;
- Multimedia tools that allow clear visualizations of complex situations;
- Research and technical staff who can use these tools in facilitating discussion and producing cohesive analysis.

4.5.4 Sandia National Laboratories (SNL)

SNL is a government-owned contractor-operated national security laboratory involved in a variety of research and development programs to help secure U.S. interests through technology. The Lab develops technologies to sustain, modernize, and protect the U.S. nuclear arsenal, prevent the spread of weapons of mass destruction, defend against terrorism, protect national infrastructures, ensure stable energy and water supplies, and provide new capabilities to U.S. armed forces.

The Lab was chosen because it is technically outside DoD by a Department of Energy's National Nuclear Security Administration sponsorship but works closely with and has a number of joint activities with the Department of Defense, and Department of Homeland Security. The Lab also works with other government agencies, industry, and academic institutions to accomplish missions in the following strategic areas:[112]

- Nonproliferation and Assessments--Reducing the proliferation of weapons of mass destruction, the threat of nuclear accidents, and the potential for damage to the environment
- Military Technologies and Applications--Addressing new threats to national security
- Energy and Infrastructure Assurance--Enhancing the surety of energy and other critical infrastructures
- Homeland Security--Helping to protect the U.S. against terrorism. The strategic objective of Sandia's Defense Systems and Assessments unit is to strengthen U.S. national security by anticipating and delivering high-impact solutions to challenging problems facing the Department of Defense (DoD).

Sandia is owned by the Department of Energy, is run by Lockheed Martin and is located at Kirtland Air Force Base. Formed in 1945, Sandia's overall mission is "to enhance the security, prosperity and well-being of the nation." Red teams have been formally part of Sandia's Information Operations Red Team & Assessments group. Each one comprises a small group (three to eight people) of computer and systems experts who believe they are the IT equivalent of a military special-operations team. The red teams provide independent assessments of information, communication and critical infrastructure to identify vulnerabilities, improve system design and help decisionmakers increase system security.[113]

SNL is involved in a variety of research and development programs to help secure U.S. interests through technology and analytical frameworks. A full description will be provided in Section 6. However, the specific laboratory used in the case study was changed to obtain the human subject matter expertise red-teaming expertise upon additional data research.

SNL is the prime contractor for the federally funded National Infrastructure Simulation and Analysis Center (NISAC). NISAC is a modeling, simulation, and analysis program that prepares and shares analyses of critical infrastructure and key resources including their interdependencies, vulnerabilities, consequences of disruption, and other complexities which includes red-teaming. NISAC is an FFRDC element under the direction of the Department of Homeland Security’s (DHS) Office of Infrastructure Protection (OIP). Sandia National Laboratories (SNL) and Los Alamos National

Laboratory (LANL) are the prime contractors for NISAC, integrating the two laboratories' expertise in the modeling and simulation of complex systems for evaluating national preparedness and security issues.

NISAC capabilities include the following:

- Dynamic Infrastructure Interdependency Simulation and Analysis
- NISAC Agent-Based Laboratory for Economics (N-ABLETM)
- Network Optimization Models
- Chemical Sector Analysis Capability
- Advanced Modeling & Techniques Investigation
- Analyses
- Fast Analysis and Simulation Team (FAST)
- Analysis of Hurricane Impacts to Infrastructure
- Pandemic Influenza Impact on Workforce and Critical Infrastructure
- Analysis for National Priorities: Tiers 1 and 2
- Western Gulf Coast Analysis
- National Hazards Analysis Tools
- Fast Analysis Infrastructure Tool (FAIT)
- Port Operations and Economic Conditions Simulators
- Spatial Infrastructure Mapping and Analysis Tool
- Telecommunications Network Simulation Modeling and Analysis Tools
- Secure Synchronous Collaboration Framework
- Knowledge Synthesis Capabilities
- Semantic Technologies for Knowledge Synthesis[114]

The NISAC webpage states that the organization contributes to secure the United States against high-consequence terrorist threats and national incidents through the use of science, technology & systems solutions. Other NISAC activities include: infrastructure modeling and analysis; decision support tools; knowledge management; fast turnaround analyses; ensure critical installation mission functions, personnel, high-value assets and infrastructure; protection of DOE/NNSA and DoD nuclear assets; ensure the function of other US government critical non-nuclear national assets, sites and infrastructure; secure U.S. borders and coasts, ports of entry such as airports and seaports, and U.S. Embassy personnel; and ensures critical installation mission functions, personnel, high-value assets and infrastructure.[115]

4.6 Data Analysis

The analytic approach consisted of reviewing all available documentation on the four organizations' red-teaming efforts; interviewing organizational leadership and red-team development experts; obtaining access to and interviewing red-team subject matter experts; recording responses to queries on their red-team design and development processes, required expertise, and identify key red-team development driver(s), requirements, design parameters, exercise steps, finding collection processes, and how the organizations distill and distribute outputs /results. After reviewing and analyzing the information in the Findings Section (6), conclusions are drawn on each red-team design and development process (Sections 7) and the organization's red team is fitted into context within the documented red-team universe. As each red team is in existence to support and improve its own blue-team system, decisionmaking, or governance/policy, red teams should share some common characteristics. A spectrum of red-team types is developed based on its primary blue-team improvement objectives and from that a red-team taxonomy is developed.

Chapter 5. Study Summary

5.1 Overview of the Red-Team Findings

The study compared different approaches to red-teaming by looking at four organizations that claim to do it: a U.S. Army training command "schoolhouse"; a nationally-recognized war-gaming center; an operational combatant command; and a government-owned, contractor-operated research center. It then compares and contrasts the design, development, use, and outputs of the red teams for common themes and best practices.

Two major approaches are identified for using red teams. One is a traditional threat emulation approach that focuses on free-form play. Interaction occurs between red and blue teams with much qualitative, and some quantitative, criteria and outputs in the form of predictive evaluations; (NWC/ONI Det model is a primary example). These red teams are traditional in the sense they have a cadre of subject matter experts; access to specialized knowledge, skills or abilities which are tailored per event; and the support of organizational leadership to market the red-team capability and be referred to by outside organizations. These red teams are developed to "play" the role of adversary and seek to test a blue team in a one or two-sided game. A series of hypotheses, all relevant background information, a scenario or a situation may be provided by the sponsor, refined by the red-team staff, and the degree of latitude between teams is provided in advance based on parameters to see what transpires. The exercise is then run and data is collected to prove or disprove the original hypothesis.

The second major red-team approach focuses on recruiting, training, and equipping internal cadres of military, civilian, and intelligence professionals to think more broadly (i.e., taking culture, economics, politics, and other social phenomena into the process) about operational and strategic problem sets. These professionals are then embedded into Combatant Command planning and integrated priority processes. These embedded red teams view operational challenges and problem sets from a different perspective to

identify courses of action that may result in unintended consequences before they are implemented or recognize courses of action that may bring about desired responses from an adversary or neutral entity in that Command's area of responsibility. These red teams also may work to provide red analytical products or develop evaluation documents that analyze red decisionmaking processes and responses. This approach seeks to embed alternative analysis inside the very structured and somewhat rote traditions of government, military, or intelligence doctrine; (i.e., the UFMCS and DIOCC/JIOC models).

Red teams also exist that try to combine the characteristics of the aforementioned approaches and apply rigorous systematic methodologies. These might be labeled "hybrid" or combination red teams that tend to take on some characteristics of both threat emulation and decision support red teams. These teams may rely on very structured methods, tools, techniques, and procedures like the SNL-NISAC vulnerability assessment approaches. The red team is but one element that is mechanistically applied only at the threat definition and adversary sequence diagramming steps to fully understand threat courses of action and determine the steps necessary to neutralize it. This red-team approach may rely on simulations and exercises which focus on logarithmic equations to calculate factors such as risks, threat, vulnerability, and assesses their characteristics as part of a larger systematic evaluation that is more holistic in nature. The red team is an embedded factor that is transparent to the overall analysis. This analytical evaluation approach delivers predictions of system or system component performance within an overall system effectiveness framework. Further, it identifies exploitable weaknesses in asset protection, physical security, or cyber attack and is designed to support management decisions regarding system upgrades in the form of defense, security, or virtualizing system assets (SNL-NISAC model).

5.2 Red-Team Similarities

In Section 6 (Findings), characteristic data was collected on all four of the red teams. Each emphasized specific attributes such as customers, approximate costs, and time analysis takes the team, outputs, and what types of adversaries are desired. In Table (5-1) below, the four case studies are compared for red-team type, customers, estimated costs, ease of implementation, and red-team flexibility is derived from ability to capture adversary behavior and apply it against a blue team.

ORGNZTN	TYPE OF RED TEAM	PRIMARY CUSTOMER BASE	RED TEAM IMPACT ON OPERATIONS RELATIVE TO COST	EASE OF IMPLEMENTING OUTPUTS	FLEXIBILITY OF RED TEAM DEVELOPMENT
TRADOC /UFMCS	Decision Support	DoD elements with emphasis on COCOMs and intelligence community agencies	Substantial downstream impact as costly stand up of university includes red team courses with more planned—graduates are embedded in COCOMs, DIOCC, and other intelligence and DoD agencies that conduct alternative analysis	Outputs are trained students that then are embedded into command elements to improve decisionmaking by using alternative analysis methods	Accounts for non state actors or whatever adversaries parent organization may encounter upon deployment, area of responsibility, etc,.
NWC/ONI DET	Threat Emulation	Federal agencies with emphasis on naval and maritime issues	Impact is less apparent tactically but there should be long term ramifications from strategic standpoint (This is difficult to measure)	Outputs are war-game findings—sponsor can accept/concur, partially accept, or ignore report	Cannot account for non state actors, tribes, criminal gangs, narco-terrorists or similar entities
DIOCC/JIOC @COCOM *X*	Decision Support/Hybrid	COCOMs	Red team analytical products are part of COCOM operations and therefore impact is immediate and measurable see Table 5-23	Decisionmaker can read reports, utilize results, modify or alter behavior to new understanding	Depends on COCOM AOR
SNL-NISAC	Threat emulation/decision support hybrid	Any governmental or private sector organization with facilities and or assets	Cost is greater than other cases here and when PPS is done its impact should be immediate and substantial	Can require large expenditures or substantial changes in doctrine, asset protection, location changes	Generally asset protection focus limits focus to facility protection but currently broadening focus to meet new customer requests

Table 5-1: Red-Team Case Studies Comparison

Each of the government red teams had champions at senior levels of parent organizations, and with the exception of the NWC/ONI-DET, were relatively new (post 9/11 and OIF) entities and stood up to address either shortcomings identified in OIF or as responses to new Presidential Directives (PD44), national security emphasis areas (DoD DIR 3000), or military refocus on different war fighting methods (Joint PUB 5.0).

The UFMCS and ONI/DET approaches both emphasized the effect their red teams had on the courses-of-action (COAs) available to both the red and blue commander. Both the SNL NISAC and the ONI/DET felt their strengths were an ability to identify, model, and apply many different threats and adversaries to a blue-team construct brought in from the sponsoring organization. As such, both red-teaming organizations were dependent on outside sponsors. Sandia National Laboratories has a steady stream of customers according to respondents; the NISAC red team has many sponsors that seek physical protection system assessments based on SNL's reputation in that field; other SNL red-team efforts such as IDART-- part of the Information Systems Analysis Center (ISAC) at Sandia National Laboratories provide information systems vulnerability assessments.

According to respondents, the UFMCS and the JIOC/DIOCC red-team models were focused primarily on training new red-teamers, embedding them in operational organizations, and thereby enhancing internal strengths in the area of decisionmaking. The red-teamers were expected to utilize their many alternative analyses methods, cross-domain tools, cultural and regional expertise, and thinking to expand the COA of the blue team. The attributes and drivers mentioned most often by interviewees and documentation for each red-team organization studied are listed below in Table (5-2).

TRADOC/ UFMCS	DIOCC/JIOC	NWC/ONI DET	SNL/ NISAC
Reduce risks (1)	Trained, educated, and practiced experts that provide an independent capability (1)	Simulation, by whatever means, of a military operation involving two or more opposing forces (1)	Defines the threat & identifies assets and prioritizing them by consequence of loss (1)
Capability to perform alternative analysis (2)	Perform adaptive planning (2)	New ways of conceptualizing the problem (2)	Identify exploitable weaknesses in protection against defined threat (2)
Cadre of staff to act as organizational mechanism to expand possible courses of action (3)	Tools to reduce an enterprise's risks and increase its opportunities (3)	Discovery of previously unknown relationships between aspects of a problem (3)	Focus on options available and associated trade-offs in terms of costs, benefits, and risks (3)
Challenge assumptions (4)	Model individual or group behavior to replicate their thinking and/or actions (4)	Identify Issues, Capabilities, & Deficiencies (4)	Systematic evaluation applied to predict physical protection system component performance and effectiveness (4)
Increase opportunities (5)	Go against accepted standards, practices, methods, by assemblage of cell with multi-disciplinary backgrounds (5)	Understand motivations for choices: Made/rejected; Refine Concepts, Doctrine, and Issues (5)	Identification of weaknesses that are used to establish the requirements for a protection system (5)
Planning and operations focus (6)	Analytic method, employed by individual analysts and collaborative teams to include alternative analysis (6)	Permit Risk-Taking; Assess Alternatives; Replicate Decision-Making Conditions; Help Prepare Military Organizations to deal with Surprises (6)	Vulnerability assessment--facility characterization-identification of protection system components in the functional areas of detection, delay, and response (6)

Table 5-2: Attributes Repeatedly Mentioned by Respondents

The two hybrid red teams, i.e., DIOC/JIOCC and SNL-NISAC combined threat emulation and other analytic tools such as vulnerability assessments with a tangible product that could impact decisionmaking.

The UFMCS really was a training institution that taught a new cadre of red-team participants and red-team leaders to operate successfully in both threat emulation and decision support environments by exposing them to a number of analytical, cultural, and operational knowledge, skills, abilities, and tools. Table (5-3) shows some of the analytical tools presented to UFMCS red-team course participants that were mentioned by respondents in the other case studies. The UFMCS red-team training develops the red-team cadres that are being embedded into the COCOM JIOCs due to the USD(I) guidance referenced later in Section 6.

The bottom two methods are the most difficult and therefore the rarest in among red-team adherents. There are some government programs that are evaluating the bottom

two tools but more information was unavailable at the time of this study. They are an area of future study.

UFMCS RED TEAMS TOOLS, TECHNIQUES, AND PROCEDURES (TTPs)	ONI/DET	JIOC/DIOCC	NISAC
Structured Brainstorming –A facilitated, focused approach that adheres to ground rules and often employs visual aids or other idea stimulating material	YES	YES	YES
"What If" Analysis –Takes as a given that an event has occurred, then 'think backwards 'to how it could have come about	YES		YES
Structured Analogies –Systematically identifies and rates analogous situations to forecast future problems and discover the most possible outcomes of a given situation		YES	
Extreme Users –A method by which a variety of participants are selected based on their expertise, or lack thereof, on the subject being discussed –"inside the box", "outside the box", and "unaware of out of the box" thinkers	YES	YES	YES
Human Factors–A method by which psychological, ethnographic, or cultural profiles are used	MINIMAL	YES	YES
Entity Mirroring –A method by which the analytic team is selected by their similarity of the modeled entity; such as hiring members of the adversary team or individuals with adversary skills or insider, first-hand knowledge	NO	MINIMAL	YES
Cultural Immersion –A method by which participants experience stimulus material designed to produce a degree of paradigm shift and inculcate a greater understanding of the adversary's perspective.	NO	NO	MINIMAL

Table 5-3: Cross Section of UFMCS Red-Team Tools, Techniques, & Procedures that were mentioned by other red-team case studies

5.3 Red-Team Differences

The case studies identified two basic types and a combination or hybrid of the two. The differences between the red-team cases can be classified into three main differences:

(1) **Decision support versus threat emulation with hybrids between the two poles**—Both UFMCS and the JIOC/DIOCC red-team models emphasized decision support while ONI/DET emphasized threat emulation. The SNL NISAC vulnerability assessment mode was a hybrid because it contained both threat emulation emphases while developing the risk assessment but its ultimate objective was to give an organization's leadership enough data to determine what systems to protect at what costs. For example, the UFMCS and DIOCC/JIOC red teams were part of the command decisionmaking staff, trusted by the command leadership elements; however, they consisted of different types

of thinkers who brought new approaches to the existing process. ONI/DET and NISAC gather sponsor requirements and then operate apart and distinctly from the sponsor to derive a series of findings.

(2) **Embedded versus externally acquired red teams—**The UFMCS and JIOC/DIOCC red-team models were embedded staff SMEs who augment the (blue team) command decisionmakers with insightful analysis of command adversaries before the command decides what COA to take. For example they may look at the leadership of Country *Z* in the COCOM area of responsibility and make a series of posits if that leader acts a certain way towards the United States. The ONI/DET and SNL NISAC red-team composition was determined by a *blue* customer. What blue concept, approach, system, strategy, or hypothesis was to be tested, and what was the red-team expertise necessary to hire and collect to properly test that blue system. The customer wants to better understand an approach and asks the ONI/DET or NISAC to model the problem. Whenever there is a marketable product involved, there will be market influences on that product to keep it relevant and desirable. How much force the market has on red-team design, application, and outputs is beyond the scope of this study but a possible future topic.

(3) **Structured versus unstructured red teams—** Structured red-team approaches involve scripts and controlled variables such as scenarios and time limits as to how much flexibility is given to the red and blue teams. The ONI/DET red-team approach was the most open to unstructured approaches while the UFMCS and the JIOC/DIOCC models were more focused on specific red elements that could impact the Commander's course of action. For example, the constraints used in ONI/DET scenarios were usually put in place to test a specific hypothesis such as "can the blue team respond to loss of its fuel supply?" or "If country A does not renew a base agreement, can the blue team still respond to a crisis in Area 1?" Unstructured red-team approaches involve more free play and concept exploration. Often, there are longer timeframes involved and more flexibility to

allow non-traditional technologies and threats to evolve, agreements with other countries/teams to occur and even the possibility of the red team building or acquiring systems to put the blue team at disadvantage. An example would be "Given an annual GDP growth rate of 5.2% and a proactive leadership with access to technology from Country E, how long would it be until Country D has the maritime forces to challenge the blue Navy in Ocean 3?" or "If a new technology is developed that allows a weapons system that has Z capability, which red team states would seek to acquire it and what would be the ramifications for the blue team in Area 4?" The NISAC physical protection system red team was much more structured into the overall methodology. The NISAC vulnerability assessment approach was strictly tied to physical security and the threats, vulnerabilities, and risks associated with such. The NISAC approach tried to fit the red-team structure into a series of equations and isolate and quantitatively define variables to minimize the uncertainty level of the findings. Once the adversary experts identified their threat definition methods, they had a series of Adversary Sequence Diagrams (ASDs) to show the expected attack process for each threat identified.

Figure (5-1) below attempts to place the four case studies into a quad chart where by the x axis is the relative level of variables under the control of the red team or red-team organizational leadership and the y axis is the degree of environmental control. All four case studies were robust enough to account for multiple types of red-team scenarios, however in comparing red teams, each model exhibited a tendency to be more or less structured and more or less operationally-focused than the other three red-team models.

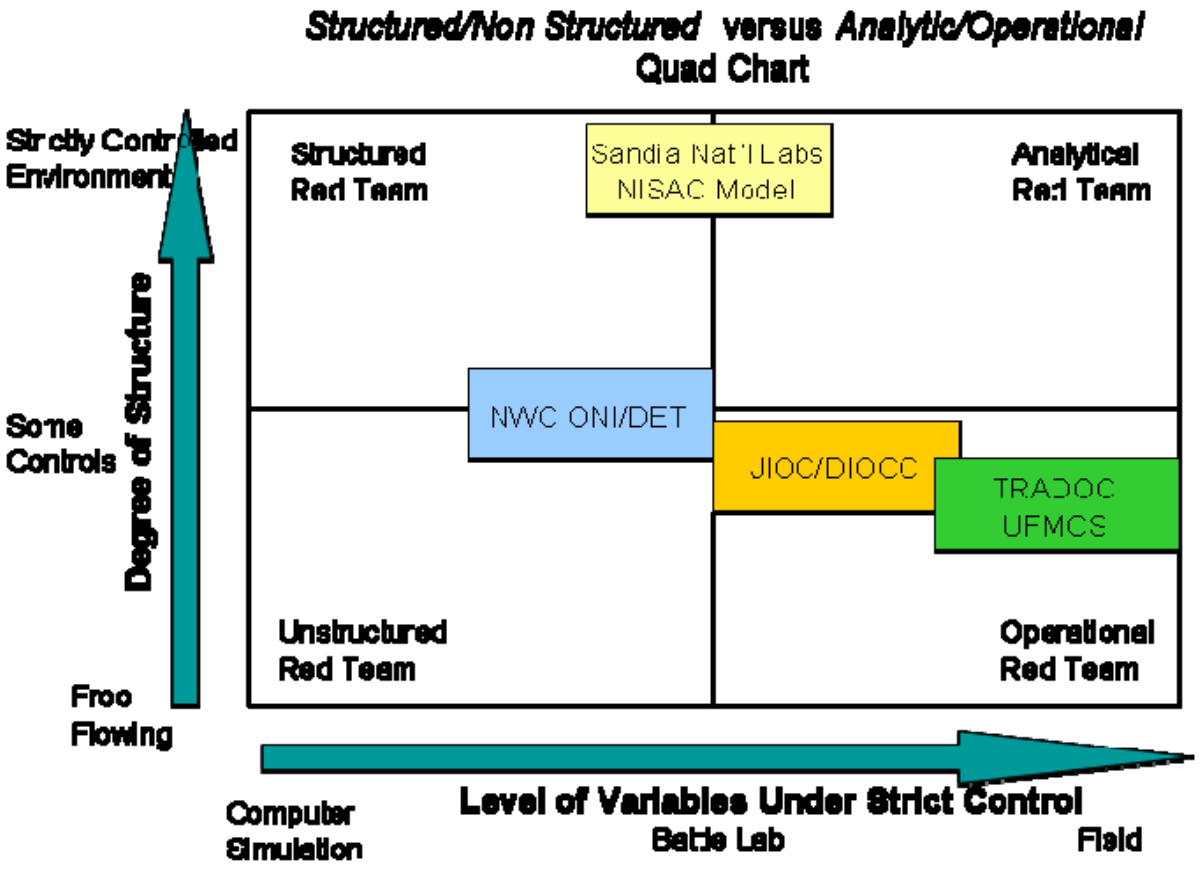


Figure 5-1: Comparison of Case Studies

For the example above, the SNL-NISAC model was the most structured and most analytical due to its reliance on strict quantitative analysis and purely strategic focus. According to respondents, the UFMCS red-team focus was on alternative analysis in an operational environment for a COCOM or other joint operations center. The UFMCS taught red- team members how to be flexible in an operational environment that may contain many variables including the groupthink or inflexible imagination of the command itself.[116] The JIOC/DIOCC red teams in actuality were the UFMCS graduates in action at a Combatant Command intelligence centers. The ONI/DET was more flexible and tended to be less structured but more capable of red-teaming strategic futures and analytic and operational blue applications.

In a comparison of the four case studies' basic time focus and costs taken from and understanding of the personnel involved by respondent and interview data, Figure (5-2)

shows how each red team compares with the other. The most personnel and time intensive is the SNL-NISAC approach (which involves more than red-teaming since it is a holistic physical protection system vulnerability assessment) which by no coincidence has a focus on purely strategic decisionmaking. The ONI/DET red-teaming is part of a war game and also requires significant investment in time and personnel tends to focus on operational and strategic threat emulation. The DIOCC/JIOC and UFMCS red teams have a symbiotic relationship and focus on quick–turn around analyses and their teams consist of three to five personnel and provide their command's with tactical and operational decision support.

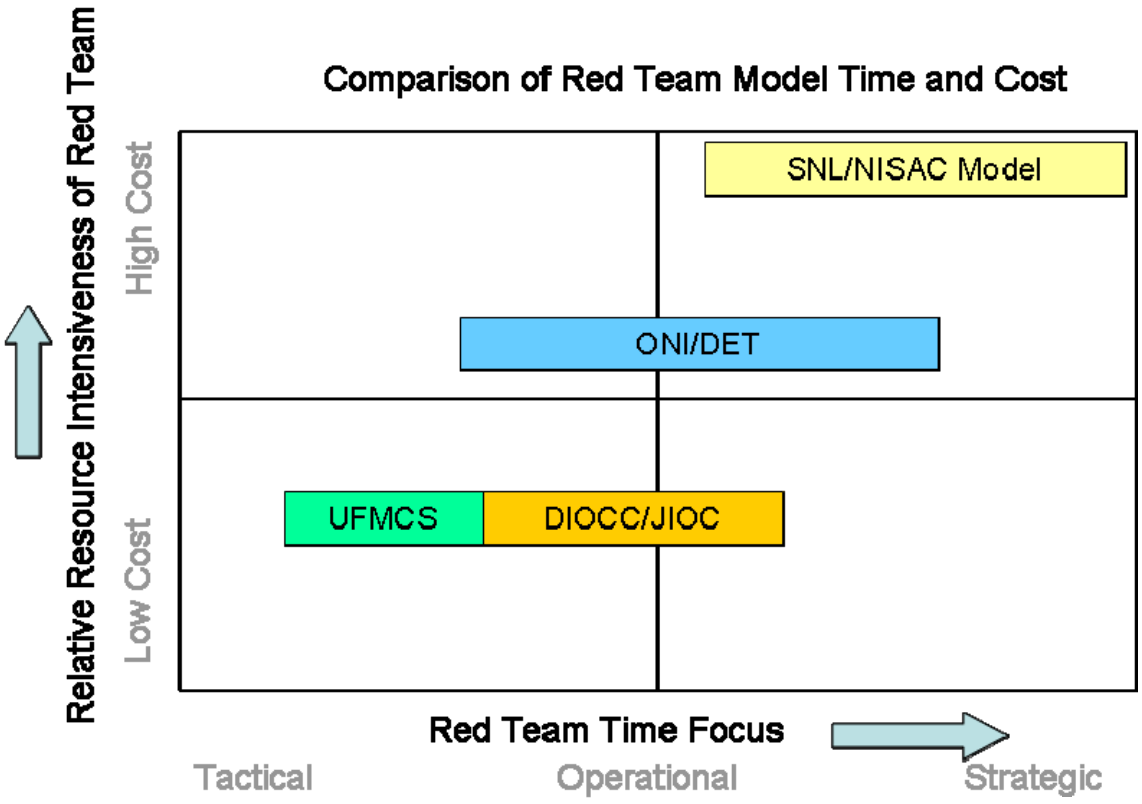


Figure 5-2: High Level Comparison of Red-Team Time and Cost Data

5.4 Comparisons of Other Key Drivers (Including *Blue Teams*)

Generally speaking, the ultimate purpose of every red team is to make the blue team better. Another approach to comparing red teams in order to develop a better

understanding of them is to examine their blue teams. Each red team is not in of itself a standalone entity. There was no formal sharing of analytic results with other types of red-team approaches across military or intelligence domains to improve blue teams. The JIOC/DIOCC red-team model is attempting to create a red-team community that shares tools, techniques, and procedures via the classified network that SNL-NISAC has no access to. The outputs of both the SNL-NISAC and the ONI/DET become the property of the sponsor and cannot be shared. As stated earlier, some red teams such as the TRADOC UFMCS red team utilized a number of other analytic tools and are placed as red-teamers including Red Team Leads in combatant command JIOCs but there was no formal interaction with an ONI/DET red team for example. There is a complete process, approach, and even acronym barrier between an FFRDC such as NISAC and the three Military/DOD red-team constructs. An example is the term *blue team* and *red team*—it is not even in the NISAC lexicon.

A possible method for comparing the disparate red teams is to compare their associated blue teams to each other. Table (5-4) below depicts the possible blue-team elements that a red team would face off against for the sake of a comparison of blue teams across the entire study. The two main types of red teams for each of the four case studies and two of the models at the extremes (e.g., threat emulation and decision support) are in the far right columns.

Blue Team Element(s) being analyzed by Red Team	Example	Perceived Ease Threat Emulation Red Teams have in analyzing	Perceived Ease Decision Support Red Teams have in analyzing
Doctrine, governance structure, operating guidelines, diffused or coalesced management structure	Combatant Command Structure, ODNI	DEPENDS –some doctrine and governance can be tested in an exercise	YES
Weapons/operating/information system hardware, facility, bases	Carrier Battle Groups, Stryker APCs, Data storage facility	YES	DIFFICULT because focus of decision support is operational environment
Strategy, operational approach, tactics	Integrated Priority List, Target list, County X weapons labs	YES	YES
Conventional &/or standard analytic approach, methodologies, tools, procedures, processes, etc.	Program Objectives Memorandum budget process, Memorandum of agreement to embed alternative analytic approaches in JIOC	SOMETIMES but it depends if a red team can be developed to test analytics in a threat emulation capacity	YES
People, staff, human characteristics, level of training, expertise, & KSAs	Soldier with rank of E-5, naval aviators, experienced intelligence analyst	DIFFICULT—human characteristics must mimic the red leadership	YES
Organizational structure, order of battle, or alignment/mix of forces	Navy Fleet, Armored Cavalry Regiment, Station Chief	YES	SOMETIMES—however, UFMCS and DIOCC deal with existing operational environ.; moving an asset into a COCOM AOR can be red teamed

Table 5-4: (Case Study) Blue-Team Emphases Areas[117]
(Derived from blue team categories in DoD Source documents)

According to respondents, the UFMCS red-team curriculum is attempting to arm the decision support element of the command with additional and non-traditional information to make a more informed decision regarding operations. This red-team approach still fits very well with a rational decisionmaking method. More information and more informed leaders make a better decision than uninformed ignorant leaders. However, the first steps towards non-linear thinking and the problems of the applications of force appear to be more apparent if the red team truly adopts the non-Western or non-linear thinking. Whether that is happening in the field is a topic for additional field work and future study.

Additionally, the NWC/ONI DET does not run any types of macro or meta-analysis on war-gaming trends or go back and validate findings from old games due to funding and time constraints. This type of information could be useful in improving games and red teams. A Meta-analysis type approach could remove specific names to protect sponsors but be available in some type of war game library depicting outputs and

findings based on ONI/ DET games design parameters and objectives. Perhaps, ONI/DET fears this may encourage more organizations to develop their own lower cost and non-sanctioned red-teaming capabilities. This is a topic for further study.

Another issue is the COCOM leadership tenure and turnover that appears to be affecting red-team adoption the limited funding and understanding of red -use. Without placing red teams in all COCOMs that want them and not formally marketing their usefulness to all COCOMs including U.S. Special Operations Command (USSOCOM), there appears to be a possible disconnect. No respondent knew what to say if red-team popularity and funding go away in the future. This possibility especially given the end of overseas contingency operations by 2013-2014 is a topic for future study.

Lastly, in the SNL-NISAC red-team methodology, after weak paths and suitable attack scenarios have been determined, a neutralization analysis is performed. This part of the analysis is performed only at facilities where there is an immediate response resulting in a face-to-face confrontation with adversaries. Neutralization analysis is an analytical term for analyzing the act of killing or capturing an adversary. It provides information about how effective the response will be under different attack scenarios and is a measure of response force capability, proficiency, training, and tactics. SNL-NISAC uses computer simulations past records of successful responses to security incidents to quantitatively predict the probability of neutralizing violent adversaries after interrupting them. However, as shown by 9/11 and the Mumbai attacks by Lashkar-e-Tayyiba (LeT) and others have proven many non-Western religious fanatics' behavior often do not fit into conventional simulations either by computer or otherwise.

Chapter 6. Detailed Study Findings

As red-team efforts exist among various intelligence and DoD establishments, since none are formally published, the ability to extract them at an unclassified level and compile them under time constraints is difficult. This study has attempted to take four and do just that. Red-teaming approaches can be classified into structured, unstructured, analytical, and operational.[118] Structured red teams are conducted strictly adhering to a defined and existing process, method, or perspective, and determine the adversarial behaviors that will emerge. Unstructured red-team approaches are free-flowing and do not adhere to any one process, method, or perspective. Analytical red teams critically assess a particular problem of interest from a hypothetical or conceptual viewpoint. Operational red teams observe, penetrate, or test an actual ("blue") asset or system.[119]

6.1 Findings Overview

The data collection effort took eight weeks and consisted of contacting the initial four organizations: the U.S. Marine Corps University, Training and Education Command's Center for Advanced Operational Cultural Learning in Quantico, Va.; National Defense University at Fort McNair in Washington, D.C.; U.S. Joint Forces Command in Norfolk, Va.; and Sandia National Laboratories in Albuquerque, N.M. The first three organizations did not do interactive red teams with SMEs.

The four organizations that were selected were based on initial survey information of military and intelligence professionals in the intelligence and defense communities and discussion with the study committee. Preliminary discussions led to the initial conclusions that the four organizations were positive organizations to start with but some might not pan out once discussions went to red-team development. Organizations that did not prove to have documented red-team approaches were

replaced with other organizations suggested by literature, intelligence professionals, and discussions with members of the first four organizations.

The initial contact with the organizations was with the front office or business offices in each of the four organizations. Called *respondent/interviewee A* types—they were asked to provide a point-of-contact for their red-team element/organization/entity.

> *"Do you know of anyone at organization X who can assist me in finding the right department or SME who has expertise in designing, developing, documenting and/or measuring red teams?"*

These questions may have been accompanied by an unclassified email with an abstract or the study prospectus. The *respondent/interviewee A* types would lead the study to *respondent/interviewee B* types who often led or ran the red-team entities. Table (6-1) below depicts the lead off questions to get to the specific data from each organization.

If type A respondents were to give a negative answer, the pursuit of red-team data at that organization would be halted. However no type A respondent in any organization in the study gave a negative answer. After type A respondents gave a positive answer, then the type B respondent was contacted. Type B respondents were generally leaders of the red team or alternative analysis organizations and were much more knowledgeable and had the organizational and red-team understanding to either refer the researcher to the desired type C respondents (the true red-team SMEs and objective of the interviews) or state that the organization did not conduct or have the red-team expertise that the researcher desired.

6.2 Initial Difficulties with Red-Teaming Organizations

The first organization, the United States Marine Corps University, Training and Education Command's Center for Advanced Operational Cultural Learning, type B respondent stated that the Center did not engage in red-team design, development, nor

implement formal red teams. The Center trains Marines on cultural and tribal issues that may be encountered but does no dynamic red-teaming as defined in the study plan. The organization was replaced by the United States Army Training and Doctrine Command (TRADOC) University of Foreign Military and Cultural Studies (UFMCS) stood up in 2006. The UFMCS did design, develop, and implement red teams.

The second organization in the study, the National Defense University National Strategic Gaming Center (NSGC) type B respondent stated that the NDU does not design, develop or implement red teams. The Center utilizes scenarios prepackaged with a series of static or single issues to work through. Since the study was begun, the NSGS has been superseded by the Strategic Policy Forum which, like the preceding NSPS, conducts exercises based on scenarios but does not utilize red teams as defined in the study.

QUESTIONS	RATIONALE	RESPONDENT TYPE (from table 6-1)
1) What is the name of defense/intelligence organization; what customers does it support; and please provide a background and experience summary or war games, blue and red teams.	Validate organization's red team efforts are within study scope; Better understanding of organization red team efforts	A
2) Does the respondent have familiarity with concept of *red-teaming?*	Validate individual's red team expertise	A,B
3) What is the conceptual understanding of the organization in terms of a systematic approach to red teams?	Does organization have formal red team development that can be understood/quantified?	B,C
4) Have there been recent war gaming instances whereby the individual had familiarity/interaction with key Non-Western doctrine or have cells/groups who regularly consulted/participate when respondent was a participant and determine how such red team participants gained "familiarity" or expertise and how this expertise is judged (quality, type, value)	Does individual have understanding of non-western red team efforts that extend concept beyond computer generated red teams?	B,C
a. Specific red team requirement	Example of nonwestern red team	C
b. Specific cultural attributes for red team	Example of cultural attribute	C
c. Requirement for other non-Western cells/organizations or outcomes	Example of exercise completion	C
5) Did after action report or game summary/findings reference or comment on cell/group robustness/adequacy in capturing realism of non-Western behaviors	Examples of outcomes	B,C
6) Please define what was successful in interviewees opinion	Red team attributes that were successful	B,C
7) Please define what failed or could have worked better in interviewees opinion	Attributes of red team that were unsuccessful	B,C
8) Please provide any other data/points-of-contact for more detailed study	Are there other organizational POCs that have insight into red teams	A,B,C
9) In respondent's opinion, what critical red team development success factors or other artifacts (such as doctrine, frameworks, CONOPs)are necessary to insure capture non-Western adversary attributes?	Critical success factors or formal framework request	B,C
10) In respondent's opinion, how should greater community maintain non-Western or non-linear adversary attributes such as networked or virtual organizations, Eastern concepts of time, of space, saving face, concept of fate.	How were specific nonwestern attributes problems worked into red team development or were they given red team products/services provided	B,C
11) Note that follow up questions to elicit information not provided or not satisfactorily provided through these questions will also be asked.	Request to contact interviewee again if necessary to clarify notes, concepts, remaining issues	A,B,C

Table 6-1: Preliminary Organization Approach

6.3 United States Army Training and Doctrine Command (TRADOC)

6.3.1 TRADOC and Red-Teaming

In the last several years, much like the private sector, the United States Army has embraced red-teaming in focusing from threat emulation to decision support. Based on recent experiences and operations in the Middle East, the Army has set up a formal educational program complete with mechanisms to insert red-team experts into the Army command strategic planning process. The Army recognizes the value of red-teaming strategies, plans, and policies before they reach the operational environment where flaws, weaknesses, and poor assumptions can be fatal to personnel, materiel, and international prestige.

Feedback from current operations and results from Joint and Army experiments have shown red-teaming to be a valuable applied methodology when used in support of planning and decision-making in a dynamic operational environment. With this in mind, the Army, along with other services and Joint commands, has decided to further develop red-team capabilities and institutionalize red-teaming processes in planning and decisionmaking.

6.3.2 The University of Foreign Military and Cultural Studies (UFMCS)

The U.S. Army Training and Doctrine Command (TRADOC) developed a joint educational program and educating professional “red-teamers” at the University of Foreign Military and Cultural Studies at Fort Leavenworth, Kan., starting in January 2006.[120]

These courses and training are part of a new program that is educating, equipping and imbedding red teams in select Joint, Service, and Army organizations. The educational part of the pilot consists of two 18-week red-team leader courses educating specially

selected students. These students are tracked and monitored as they perform red-team functions in the organizations and operational units in which they have been imbedded.

According to Spade (2005), the intent is to enable a force-wide red-teaming capability and to assess both the utility of red-teaming and the quality of the curriculum. Like other advanced studies programs, the course involves a rigorous curriculum with extensive readings, case studies and practical exercises in a seminar setting.[121] Zahn (2005), in a brief from the office of TRADOC's Deputy Chief of Staff for Intelligence states:

> "Our commanders and staffs routinely operate under conditions of extreme complexity and uncertainty, and our goal is to help them improve planning and decision-making under those conditions. We define red-teaming as a function performed by educated team members who can independently review and challenge assumptions, plans and other staff processes in the context of the operational environment and from our partners' and adversary's perspectives."[122]

Key TRADOC respondents who run the course state that the objective of the program is about getting beyond American ethnocentricities and training officers to think about problems from others' perspectives, whether adversaries or coalition partners. Zahn (2005) further states:

> "The mission of the University of Foreign Military and Cultural Studies is to provide the education, training and practical experience necessary to enable that function. To do that, we think we have to provide red-team leaders with intellectual skills and tools not typically resident within the officer or (noncommissioned officer) corps. The Army and the Joint force are unmatched in doing things right. We have the best trained and best equipped force in the world with training, equipment and processes designed to make sure we do things right, but the question is, are we doing the right things? Red-teaming is about helping the commander do just that."[123]

6.3.3 UFMCS Curriculum

TRADOC UFMCS proponents believe with culture (now called *human terrain* in DoD lexicon) having an ever-increasing impact on military operations, the University prepares commanders and their staff with trained officers and non commissioned

officers (NCOs) that possess the knowledge, skills and resources to approach problems by considering non-Western perspectives and thereby reduce operational and political risk. The University curriculum includes a broad set of topics, many of which cannot be found in any current professional officer or noncommissioned officer education systems. UFMCS emphasizes both Western and non-Western military theory because organizers believe the graduate red-teamers must understand both to frame the problem and predict points of friction (Zahn, 2005). Included in the coursework, is a class on the science of semiotics – that is, cross-cultural communication and understanding the subtleties of signs and their meaning. The curriculum relies heavily on historical and contemporary case studies because they provide no shortage of vehicles where, given known outcomes, the trained red-teamers can examine and attempt to understand the perspectives of all parties involved.[124]

UFMCS pilot courses include:

Red team Leader Course (18 weeks) – intended for leaders of red teams pulled from a unit of action, unit of employment- begun in January 2006.

Red Team Member Course (six weeks) – intended for subordinate members of a red team consisting of officers pulled from an Army command element. Initial course start date was spring 2006.

Red Team Practitioner Course (two weeks) – intended for mentors and subject-matter experts assigned to support operational red teams. Key findings for the UFMCS are below in tables (6-2), (6-3), (6-4), (6-5), (6-6), and (6-7).

KEY COURSE OBJECTIVES	RED TEAM COURSE FUNDAMENTAL SOURCES	MENTIONED BY RESPONDENT
Reduce risks and increase opportunities	Defense Science Board (DSB) Report on Red teaming stated goal of red teams is to reduce an enterprise's risk and increase its opportunities	Yes
Alternative analysis	The DSB further states-"…aggressive red teams challenge emerging operational concepts."	Yes
Organizational mechanism	Robb-Silberman report on Iraqi WMD-widely recognized need for alternative analysis drives many to propose organizational solutions such as "red teams". Indeed, the Intelligence Reform and Terrorism Prevention Act mandates the establishment of such mechanisms terrors in planning, and avoiding patterns during operation to ensure that analysts conduct alternative analysis.	Partial
Challenge assumptions	Lessons learned during combat operations illustrate importance of continually challenging assumptions, identifying errors in planning, and avoid patterns during operations.	Yes
Challenge enemy assumptions	USJFCOM Iraqi Perspective Project re: Saddam Hussein's convictions that regime would survive war	Yes

Table 6-2: Key UFMCS Red-Team Course Objectives and Sources

According to respondents, the Army looks at red-teaming as a method to ensure rigor in its operational decisionmaking and mission planning at the command, division, and brigade levels. Trained red teams embedded in units can challenge operational plans before they are carried out. Army TRADOC has set up the Red Team Leader (RTL) and Red Team Members (RTM) courses at the UFMCS to expose a growing cadre of mid grade and junior officers what it believes are the tenets of effective red-teaming. Table (6-4) below outlines the overall curriculum objectives of the two RT courses.

Red Team Leader Development 18 week RT Leader and 9 week RT Members Course Objectives
Training, education, and experience with red teaming TTP to include how to set up and operate a red team; this includes exposure to, study, and research:
Red team Tactics, Techniques and Procedures, The application of diverse theories;
Application of the proceeding subjects into various contemporary environments;
Doctrine relating to war-gaming, coalitions, and adversaries;
Exposure to case studies and actual operations and planning
Regional military and civilian? cultural anthropology;
Practiced in looking at complex situations and developing a theory of how they work--
A cultural anthropology toolkit that helps the staff ask the right questions in order to operate within cultural contexts
Communication and negotiation skills that enable the RT to challenge the staff and the plan without being a disruptive force

Table 6-3: Key UFMCS Red-Team Curriculum Objectives

The emphasis is on addressing two key gaps in Army decisionmaking: (1) the cultural, organizational, political, military, and economic blind spots for decisionmaking that may exist at the divisional, brigade, and battalion levels; (2) Fundamental changes in national security, U.S. military, and Army doctrine (i.e., Presidential Directive (PD-44), Joint Military Publication Military Decisionmaking Process (MDMP)/ FM 5-0, Planning/Joint Publication 5–0L, and US Army Field manual 3-07), have fundamentally changed the roles and missions of the U.S. military. These documents have formalized the addition of nation-building into Army responsibilities, inserted coalition relationships into Army planning, put civilian interagency coordination at the center of Army capabilities, and put a focus on somehow *converting* violent conflict dynamics into

processes for constructive change.[125] Interviews with UFMCS leadership, staff, and students validated a concerted attempt to greatly expand an operational unit commanders' staff with cultural and alternative analytical tools. Additionally, there was a palpable excitement with interviewees that they indeed had new insights on 21st Century adversaries.

Along with the difficult counterinsurgency missions in Operation Iraqi Freedom, Operation Enduring Freedom, and Afghanistan-Pakistan operations, these documents have complicated the Army's ability to plan, conduct, and succeed at what used to be traditional offensive and defensive armed warfare. Table (6-4) below lists the relevant new directives and their complex requirements for the Services and especially the Army. In comparison to past conflicts which could be divided into strictly offensive and defensive operations, these new requirements have greatly complicated training and TRADOC is examining its courses to find ways to broaden its officer and enlisted student minds.

These new drivers of strategy below are tangible directives and instructions excerpts that emphasize new roles away from traditional war fighting and towards international partnerships, coalition building, national infrastructure maintaining, and stabilizing regimes. These new roles have affected the military services in that their primary goals are to recruit, train, and equip their personnel. If their personnel are untrained for new roles and missions, they will be less likely to succeed.

TRADOC UFMCS DRIVERS/RQMTS	
US Army Field Manual 3-07, "Whole government approach"	1-17. A *whole of government approach* is an approach that integrates the collaborative efforts of the departments and agencies of the United States Government to achieve unity of effort toward a shared goal. A whole of government approach is vital to achieving the balance of resources, capabilities, and activities that reinforce progress made by one of the instruments of national power while enabling success among the others. It relies on interagency coordination among the agencies of the USG, including the Department of Defense, to ensure that the full range of available capabilities are leveraged, synchronized, and applied toward addressing the drivers of conflict and reinforcing local institutions to facilitate achieving sustainable peace. Success in this approach depends upon the ability of civilians and military forces to plan jointly and respond quickly and effectively through an integrated, interagency approach to a fundamentally dynamic situation. Accomplishing this requires a willingness and ability to share resources among USG agencies and organizations while working toward a common goal. These resources—financial, military, intelligence, law enforcement, diplomatic, developmental, and strategic Communications—are often limited in availability and cannot be restricted to use by a single agency, Service, or entity. To achieve the broad success envisioned in a whole of government engagement, all must be integral to unified action. All are elements of the whole of government approach.
US Army Field Manual 3-07; :integration of planning"	1-18. To that end, all actors involved in unified action are integrated into the operation from the onset of planning. Together, they complete Detailed analysis of the situation and operational environment, develop integrated courses of action, and continuously assess the situation throughout execution. These actions ensure that the various capabilities and activities focus on achieving specific conflict transformation goals in cooperation with

	host-nation and international partners. A coherent whole of government approach requires early and high-level participation of both national and multinational civilian and military participants. This process necessitates active dialog and reciprocal information sharing with intergovernmental and nongovernmental organizations, the host-nation government, and the private sector, when necessary.
US Army Field Manual 3-07; Focus on "*conflict transformation"*	1-23. Conflict transformation focuses on converting the dynamics of conflict into processes for constructive, positive change. *Conflict transformation* is the process of reducing the means and motivations for violent conflict while developing more viable, peaceful alternatives for the competitive pursuit of political and socioeconomic aspirations**.** It aims to set the host nation on a sustainable positive trajectory where transformational processes can directly address the dynamics causing civil strife or violent conflict. It seeks to resolve the root causes of conflict and instability while building the capacity of local institutions to forge and sustain effective governance, economic development, and the rule of law.
US Army Field Manual 3-07; "*capacity building"*	1-35. Building institutional capacity in the host nation is fundamental to success in stability operations. *Capacity building* is the process of creating an environment that fosters host-nation institutional development, community participation, human resources development, and strengthening managerial systems. It includes efforts to improve governance capacity, political moderation, and good governance—ethos as well as structure—as part of broader capacity-building activities within a society. Supported by appropriate policy and legal frameworks, capacity building is a long-term, continuing process, in which all actors contribute to enhancing the host nation's human, technological, organizational, institutional, and resource capabilities.
National Security Presidential Directive 44 (PD44)	In 2005, President George Bush signed National Security Presidential Directive 44 (NSPD-44). NSPD-44 outlines the President's vision for promoting the security of the United States through improved coordination, planning, and implementation of reconstruction and stabilization assistance**.** This policy is significant for two reasons: it was his administration's first attempt at defining national policy for interagency integration, and it was the first time that any administration implemented interagency policy focused on stability operations. In addition, NSPD-44 formally acknowledged that the stability of foreign states served the broader national interests of the United States, recognizing stability operations as a necessary capability of the Federal government.
Department of Defense Directive 3000.05 (DOD-DIR-3000.05)	Also in 2005, the Secretary of Defense signed DODD 3000.05 providing the military force with definitive guidance to conduct stability operations. It outlines Department of Defense policy and assigns responsibility for planning, preparing for, and executing stability operations. It is part of a broader USG and international effort to establish or maintain order in states and regions while supporting national interests. Most importantly, however, it establishes stability operations as a core military mission on par with combat operations. DODD 3000.05 also emphasizes that many of the tasks executed in a stability operation are best performed by host-nation, foreign, or USG civilian personnel, with military forces providing support as required. However, the directive clearly states that, in the event civilians are not prepared to perform those tasks, military forces will assume that responsibility. Finally, the directive describes the comprehensive purposes supporting these tasks: □ Rebuild host-nation institutions, including various types of security forces, correctional facilities, and judicial systems necessary to secure and stabilize the environment. □ Revive or build the private sector, including encouraging citizen-driven, bottom-up economic activity and constructing necessary infrastructure. □ Develop representative government institutions. 1-74. In addition, DODD 3000.05 defines the goals for stability operations. The immediate goal, consistent with initial response efforts, is to provide the local populace with security, restore essential services, and meet humanitarian needs. Long-term goals that reflect transformation and foster sustainability efforts include developing host-nation capacity for securing essential services, a viable market economy, rule of law, legitimate and effective institutions, and a robust civil society.
US Army Field Manual 3-07	2-1. Full spectrum operations apply to the joint force as well as Army forces. The foundations for Army operations conducted outside the United States and its territories are reflected in the elements of full spectrum operations: continuous, simultaneous combinations of offensive, defensive, and stability tasks. These combinations are manifested in operations designed to seize, retain, and exploit the initiative using the mutually supporting lethal and nonlethal capabilities of Army forces. This is the essence of full spectrum operations, representing the core of Army doctrine. In full spectrum operations, the emphasis on the individual elements changes with echelon, time, and location. No single element is more important than another is; simultaneous combinations of the elements, constantly adapted to the dynamic conditions of the operational environment, are key to successful operations.
US Army Field Manual 3-07	2-17. Perception is also a major factor for military forces; the actions of Soldiers, both positive and negative, influence how the local populace perceives the military. Therefore, in all actions, leaders focus on managing expectations and informing the people about friendly intentions and actions. This is accomplished through specific nonlethal means: information engagement. Commanders use information engagement to inform, influence, and persuade the populace within limits prescribed by international law. In this way, commanders enhance the legitimacy of the operation and the credibility of friendly forces. 2-18. Effective, accurate, and timely intelligence is essential to successful full spectrum operations. This is especially true in stability operations where the ultimate success or failure of the mission often depends on the effectiveness of the intelligence effort. In operations conducted among the people, tailored intelligence facilitates understanding of the operational environment while emphasizing the local populace, the host nation government, and the security apparatus of the state. Commanders require accurate and timely intelligence to retain the initiative during stability operations.
Department of the Army Pamphlet 10–1	1–4. Changing National Military Strategy *a.* The President's National Security Strategy sets forth national security goals designed to ensure economic stability, territorial security, freedom, and democracy for all citizens. A National Military Strategy prepared by the Chairman of the Joint Chiefs of Staff in coordination with the service Chiefs of Staff and the Combatant Commanders of the unified commands is then defined to account for changing world events. Our current assessment cites four dangers facing the nation: proliferation of weapons of mass destruction; regional, ethnic, and religious conflicts; stability of democratic reform in former Soviet Union, Eastern Europe, Latin America, and elsewhere; and achievement of national security interest, and those of our allies, in a way that adequately incorporates economic concerns. Considering these dangers, our National Military Strategy has evolved from that of "containment" to that of "engagement," "partnership," and "prevention." The Army is a substantial contributor to the National Military Strategy in that it provides land forces for: Warfighting Deterrence Small Scale Operations *b.* To ensure the Army's fulfillment of its role in this National Military Strategy, the Secretary of the Army and the

	Army Chief of Staff established a vision for the Army on its journey to the 21st century. Six imperatives guide the Army in management of change while ensuring continuity and growth.
Military Decisionmaking Process (MDMP)/ FM 5-0, Planning	The military decisionmaking process is a planning model that establishes procedures for analyzing a mission, developing, analyzing, and comparing course of action against criteria of success and each other, selecting the optimum course of action and producing a plan or order. The MDMP applies across the spectrum of conflict and range of military operations. Commanders with an assigned staff use the MDMP to organize their planning activities, share a common understanding of the mission and commander's intent, and develop effective plans and orders.
Joint Publication 5–0	Doctrine for Planning Joint Operations augmented by other service doctrinal and other planning related publications provide the Details of how to plan military operations during deliberate planning
Field Manual 5-0, Army Planning and Orders Production, January 2005	Serves as the primary source for the Army's planning system. Red team members must understand this planning process in order to know how and when they can influence the planning process. Joint Publication 5–0, Doctrine for Planning Joint Operations augmented by other service doctrinal and other planning related publications provide the Details of how to plan military operations during deliberate planning.10 Field Manual 5-0, Army Planning and Orders Production, January 2005, serves as the primary source for the Army's planning system. Red team members must understand this planning process in order to know how and when they can influence the planning process. Red teams supports planning for all types of operations, across the spectrum of conflict and during all phases of an operation.

Table 6-4: Key UFMCS Red-Team Course Drivers

These drivers have forced the Army and other Services to go back and re-examine their training and doctrine. The new strategic reality of civilian partnerships, coalition and host nation joint planning, nation building, converting conflict into positive change, and de-emphasis on killing the enemy and preventing being killed, has forced the Army to completely revamp its training, doctrine, and ultimately, its people according to respondents at UFMCS and review of doctrine. A problem is that the Army has the people, equipment, doctrine, and some thinking from the last century when warfare was versus state-sponsored uniformed professional armies. Table (6-5) outlines the key design objectives the red-team course designers sought to incorporate into the UFMCS curricula to begin to address this gap between the Army of the last century and the Army needed today.

KEY DESIGN PARAMETERS/FOCUS AREAS/FUNDAMENTAL METHODOLOGY[126]
Decision support focus
Support commander's planning process
Gary Kline-Method "The Pre-mortem" --assumes plan is complete and it failed--WHY???
Planning and operations focus with goal to improve decisionmaking in planning and operations (alternatives) by: --Broaden understanding of the variables found in the Operational Environment (OE) and stakeholders' perspectives affecting planning and operations.
Critical review and analysis focus with goal to improve decisionmaking and problem solving by: --Performing independent critical reviews and analysis of concepts, doctrine, and new organizational designs --Insuring OE accounted for in experiments, concepts, and war games.
Intelligence focus with goal to improve understanding of enemy, estimates, and better synchronization of intel and ops by: --Think like the enemy --Account for culture and other variables of the OE --Conduct alternative (competitive) analysis --Ensure enemy is appropriately war gamed.

Table 6-5: Key UFMCS Red-Team Design Objectives

6.3.4 UFMCS Red-Team Process

The actual RT process for the students is outlined below in Table (6-6). Items 1 through 3 are the initial process for selection. Items 4 through 11 are the RTL walkthrough from receipt of task through execution of the plan. Items 12 through 17 are completed after the mission but prior to course completion. The red colored items are the actual red-team actions practiced and honed during the course. The key element is the red team is inserted into the commanders planning processes as shown at the strategic level in the Military/DoD red-team model in Section (2) and in greater detail in the Malone and Schaupp model in Section (2) and (3).

PROCESS STEPS	RATIONALE
1 Commander of Division or Corps (sometimes brigade) orders individ. to be red team (RT) leader and receive training to do so.	Identify strength in RT approach or weakness in existing planning processes
2 Commander picks 2-3 Army staff college grads to be designated RT staff on his J1 planning or J2 intelligence branch of brigade/division/corps	Set up of RT element within Army division or corps
3 Send individ. off to a 9-18 week course at UFMCS	Incorporation of RT course into individual's training plan
4A Blue staff actions include: • Attend mission brief/review mission guidance and order. • Update staffing estimates • Develop staff planning timeline based on time available from receipt to execution. • Commander issues initial planning guidance for planning (e.g. abbreviated planning process). 4B Red team actions include: • Attend mission brief/review mission guidance and order. • Begin data collection and identification of information need to support operational analysis of 12 variables including *culture* as an internal team product. • Based on staff planning timeline, develop preliminary RT internal product timeline (e.g. when operational analysis is to be completed). • Receive/ recommend preliminary RT initial guidance from org. commander. • Determine extra-org. requirements—if any.	Receipt of Mission
5A Blue staff actions include • Receipt of Mission perform initial /Mission Analysis: • Analyze leadership order. • Perform initial intelligence preparation of the battlefield (IPB). • Determine specified, implied, and essential tasks. • Determine available assets. • Determine constraints. • Identify critical facts and assumptions. • Perform risk assessment. • Determine initial Commander's Critical Information Required (CCIR) and Essential Elements of Friendly's Information (EEFI). • Determine the initial Intelligence, Surveillance, and Reconnaissance (ISR) plan. • Update operational timelines. • Write the restated mission. • Deliver a mission analysis brief to Commander. • Approve the restated mission. • Develop the initial Commander's (CDR) intent. • Review facts and assumptions. 5B Red team actions include: • Independently from the staff, identify alternative end-states for US, coalition, and the adversary - based on Operating Environment (OE) variables and cultural analysis of Operational Requirements (OR) • Participate in planning • Receive/ recommend preliminary RT initial guidance from commander. • Independently identify the friendly, enemy, and coalition Centers Of Gravity. • Assist in identification of specified, implied, and essential tasks. • Provide insights to validate assumptions.	Mission Analysis

• Assist and ensure end state definition for US, enemy, coalition and other players. • Attend mission analysis brief. • Continue OE and cultural analysis for use in Course of Action (COA) Development.	
6A Blue staff actions include • Analyze relative combat power • Generate options • Array Initial Forces • Develop the Concept of Operations • Assign Headquarters • Prepare COA Statements and Sketches • Conduct Course of Action Briefing • Write the restated mission. 6B Red team actions include: • Monitor staff development of COA. • Analyze OR • Independently develop COA based on projected objective, doctrine, capabilities, geography, and culture. • Identify potential 2nd and 3rd order effects of friendly COA and actions.	Course of Action (COA) Development
7A Blue staff actions include • Gather the tools • List all friendly forces • List known critical events and decision points • Determine evaluation criteria • Select the war game method • Select a method to record and display results • War game the battle and assess the results 7B Red team actions include: • Help staff to decide if adequate measures are in place to measure success and how/who will provide input to the measurement. • Monitor war game to help ensure accuracy - • Ensure realistic capabilities are maintained • Evaluate appropriate actions and results • Balance operational requirements with other elements • Assist staff by serving as war game "umpire."	COA Analysis
8A Blue staff actions include • Conduct a COA Advantage and Disadvantage Analysis • Compare COAs • Develop a recommended COA 8B Red team actions include: • Monitor to ensure RT COA accounts for each of the identified OE variables	COA Comparison
9 Red team actions include: • If directed, conduct order's crosswalk to identify gaps, disconnects, or vulnerabilities to the plan based on critical review of the prepared order and staff annexes and appendices. • Linkage of staff actions to the end state Key Points/(key plan elements) (Red teams do not normally produce a separate staff product) • The Red team's value added is measured by the staff producing a better staff product and identification of alternatives to the staff and Commander (The Role of Red teams is dependent on the commander's guidance and culture of the unit)	Operation Plan/Operation Order (OPLAN/OPORD) Production & Briefing to Organization Commander
10 Conduct Mission Rehearsal Exercises (MRX)	MRX
11 Execute mission	Execute
12 Completion of course and should result in cadre/cell with trained RTers	Course completion
13 In interim; may have to use Army reservists, adhoc teams or leverage JIOCs, DIOC, COCOM teams who have in-Theater experience and understanding of problems	Augment shortage of RT in Corps/Division/Brigade staff ranks
14 Develop red team leaders and access Red team Central on line via unclass. Internet (SIPRNET)	Reinforce RT approaches
15 Add'l Army training to ensure development. of field grade officers with RT peers	Do not forget regular Army or other agency training
16 Take add'l UFMCS lessons include negotiation skills, Heisenberg's theorem-enemy gets a vote; SME's come in to lecture; courses in Anthropology, Swest Asia or other AOR studies depending on assignment; Communications; Read "Management of Savagery"; al Qutb, Koran; Hadiths; "Reliance on the Traveler"; Koranic Way of War; etc	Intro to analytic methodologies
17 Understand four ways of seeing: see us see ourselves, see them see themselves (r-r, r-b, b-r, b-b) Understand cultural variables	Simple paradigmatic framework
0 Reading list	RT handbook reading list (avail in appendix)

Table 6-6: Key UFMCS Red-Team Exercise Process Steps[127]

6.3.5 UFMCS Red-Team Challenges

According to UFMCS respondents and Army doctrine, during the planning and execution of operations across the spectrum of conflict, commanders and staffs routinely and continuously monitor and evaluate the current situation, the progress of an operation and evaluate the operation against measures of effectiveness and performance. In essence, assessment determines whether a program or mission is being accomplished and answers the simple question – "*Are we winning and/or accomplishing our mission*?"[128] Red-team leaders and staffs review plans and independently assess alternatives and other approaches that take into consideration partners, adversaries, and other in-theatre actors (such as coalition partners, non-combatants, etc.). However the actual process is often not easy and there are challenges and preconceived notions about enemies, one's own capability, intelligence values, and logistical resupply that must be assessed by the UFMCS-trained RT graduate. Some of the challenges are listed below in Table (6-7).

COLLECT FINDINGS/CRITICAL QUESTIONS	CHALLENGES
When should the Red team engage in the planning process?	Red teams face a number of challenges to provide commanders an independent capability to fully explore alternatives to plans, operations, concepts, organizations, and capabilities in the context of the operational environment and from the perspective of partners, adversaries, and others.
How should the Red team engage? What are the expected deliverables or outcomes? What level of leadership should they report to?	Remaining Independent but Accountable. While independent of the senior staff elements, red teams rely on staffs to provide them information and must work with staff members to resolve issues, insights, and observations impacts on groupthink and popular beliefs.
What linkage should the red team have within the staff? For example, is it expected that the red team observe or actively participate in the wargaming process or develop alternatives on their own?	Inherent tension with the staff. Given the red team's mission, there is an inherent tension with the staff who may view the red team's efforts with suspicion. The Commander must endorse the red team's mission, and the red team must carefully weigh which items require elevation to the Commander.
What information does the red team need and is it available inside or external to the unit? Are their restrictions on the dissemination of information? What reach back capability does the team require?	Group Think versus outside independence. While the red team should be an independent staff entity, it lives and works within the unit or organization. The team must balance it abilities to be part of the team; cooperatively working to accomplish the mission, while remaining immune to groupthink.
Was commander's Corps/division/brigade goals met?	While the deliberate planning system describes a linear thinking process (e.g. Mission Analysis consists of 17 steps), no single red team tools/techniques/procedures can fit all problems.
Was planning process robust enough when conditions changed?	FM 5-0 describes the Military Decisionmaking Process in great detail and also discusses the challenges to effective planning; specifically addressing groupthink. The manual further notes, "the leader should assign individuals to independently examine the group's decision processes". - a capability inherent to a red team.
What options were not considered and why not?	RTs broaden the understanding of the operational environment from alternative perspectives, and identifying gaps, vulnerabilities, and opportunities.
Which old assumptions became fact?	Identification of branches and sequels; Identification of measures of effectiveness; Enables a learning organization; Avoid conventional patterns of operations.
Center for Army Lessons Learned red team Central on line Review doctrine continuously, the new red team cadre knows Army doctrine staff at TRADOC; review doctrine provide updates via	Red teaming is largely an intellectual process which incorporate the following characteristics: • To be effective, red teams must have the Commander's confidence, support, and direction to effectively complete its tasks. • To be effective, red teams balance the requirement to be independent of the staff processes in

formal review process	order to provide alternative views and avoid group think while remaining engaged with the staff. • Red teaming is confrontational – challenging existing thought processes and estimates without being confrontational to individuals or staffs. • Red teaming is more an art than a science – requiring red team members to possess superb critical and creative thinking skills and an understanding of the barriers and symptoms of poor thinking. • Red team best practices apply to assigned, ad hoc, or combined teams. • Red teaming is not process driven but effective red teams must understand the MDMP and culture of the unit in order to contribute to effective decisionmaking.

Table 6-7: Key UFMCS Red-Team Findings' Key Questions and Challenges[129]

According to TRADOC respondents, red-teamers must help the commander's staff determine if they are assessing the right things, provide an independent review to define adequate assessment resources and procedures, which in turn, helps the staff determine the next right thing to do. Additionally;[130]

- Red teams offer perspectives of how the enemy might assess their operations and help the staff account for coalition or mission partners' perspectives to ensure a common understanding of the metrics used in the assessment process.
- Red teams provide the commander an independent capability to conduct critical reviews and analysis to include a review of a program, organization, or unit's assessment system.
- The value added of a red team in the assessment process occurs when:

  --Commander and staff established metrics properly focused on the end-state and adequate resources allocated to obtain the data for assessment.
  --Red teams provide another perspective on the assessment process to ensure we evaluate the right things. Offers alternative perspectives of how the enemy views his progress.
  --Offers perspectives of how coalition partners view assessment and whether there is a common understanding of the metrics used.

6.3.6 UFMCS Red-Team Measurements/Metrics against the DoD/Military Red-Team Model

When assessing red-team success, it is important to understand the limitations of the red team and where it fits into the corps/division/ brigade decisionmaking hierarchy. Additionally, some commanders discount the concept of an internal independent

assessment group making judgments from an enemy perspective; some commanders do not fully understand the value or may overstate the value of the RT. This danger was repeatedly mentioned by respondents. It is too early to see if these UFMCS red-team graduates have sufficiently addressed the concerns above. Ideal contributions of successful red teams are listed below to provide a better understanding of the outputs and the focus areas impacted according to the 2007 UFMCS Red Team Handbook provided by TRADOC.[131]

DISTILL OUTPUTS/RESULTS	FOCUS AREA
Did we accomplish commander's division goals?	Operations and Planning, Critical Review and Analysis
Did conditions change?	Intelligence, Critical Review and Analysis
What options were not considered?	Critical Review and Analysis
Which old assumptions became fact?	Critical Review and Analysis
Center for Army Lessons Learned	Intelligence
Red team Central on line	Operations and Planning, Critical Review and Analysis, Intelligence
Review doctrine continuously, RT'ers know Army doctrine staff at TRADOC; review doctrine provide updates via formal review process	Intelligence, Critical Review and Analysis

Table 6-8: Distillation of UFMCS Red-Team Outputs/Results/Metrics by Focus Area[132]

Ultimately, upon completion of the mission, the operational red team must answer a number of questions for assessing the commander's mission success or failure and the usefulness of their review on that success:

- Are the proposed measurements of effectiveness clearly linked to the strategy, plan, or mission or end state?
- Does the measurement have a clear start point (baseline) in which to measure progress?
- Does the measurement system incorporate higher headquarters metrics? Are the unit's tasks developed to local conditions?
- Has the coalition or interagency agreed to the assessment measures? If not, what are the implications?
- Who has primary responsibility for assessment? Has the task (who, what, when, where) been established?
- For combat operations, has the assessment been included in the unit's Commander's Critical Information Requirement (CCIR)?
- Are the established assessment measures in concert with higher headquarters efforts and understood by subordinate headquarters?
- Do the metrics reflect a cultural sensitivity, whereby important things are measured? [133]

The key point the UFMCS subject matter expert respondents pointed out was the Red Team Leader and staff must be linked to a realistic strategy and plans by the commander; Then the team can play a role as an effective assessment system which links quantitative and qualitative evidence providing a powerful tool to not only determine progress but also enabling commanders to make real time adjustments to their plans. Red teams can assist the staff in determining whether their assessment program is focused on the right things and help them determine the next right thing to do.[134] The embedded UFMCS graduates are recently deployed and only U.S. Pacific Command (USPACOM) had UFMCS graduates who were supplying red-team products to the classified Intelink at the time of the case study interviews.

According to respondents, the UFMCS red-team curriculum is attempting to arm the decision support element of the command with additional and non-traditional information to make a more informed decision regarding operations. This red-team approach still fits very well with a rational decisionmaking method. More information and more informed leaders make a better decision than uninformed ignorant leaders. However, the first steps towards non-linear thinking and the problems of the applications of force appear to be more apparent if the red team truly adopts the non-Western or non-linear thinking. Whether that is happening in the field is a topic for additional field work and future study.

6.4 Naval War College/Office of Naval Intelligence (ONI) Detachment (DET)

6.4.1 War game Origins of NWC Red Teams

War games and their associated red-team development have been part of the Naval War College Gaming curriculum since 1887. According to the Naval War College (NWC) website, these war games are vehicles for generating, testing, and debating strategic and operational concepts and for exercising military and civilian decisionmakers in maritime and joint warfare.[135] As war-gaming is an effective

technique for creating a decision-making environment that fosters education and understanding for students and operational staffs, provides insights, and generates issues for further study, the red-team component of them becomes more crucial. Groups of games set in the same theater or exploring the same or similar issues can help players to understand the dynamics of war fighting and may suggest possible trends or tendencies which could be exploited in real-world situations. Depending on scenarios, red teams can be a crucial component of NWC war games.

Based on their website, the NWC War-gaming Department think of themselves as one of the world's premier *gaming* organizations, conducting approximately 50 games yearly in support of internal College needs and externally generated requests from various branches of the Defense and Navy departments, operational commands and civilian agencies, including the Office of the Vice President of the United States, the Joint Chiefs of Staff, and the Secretary of the Navy. To support the objectives of each game's sponsor including red-team design, the War-gaming Department employs a wide variety of gaming techniques ranging from complex, multi-sided, computer-assisted games to simpler, single-sided seminar games, and game foci can range from broad national strategies to the specifics of tactics. Most games take place at the College, but some are conducted off site.

According to respondents, the Office of Naval Intelligence (ONI) has a detachment of experts and analysts at the War-gaming Department to assist NWC in designing and developing red teams that require some interactive and complex qualities for specific types of games. These specific games have a requirement for high flexibility, exploratory, and/or are applying assessment methodologies that need an interactive adversary or replication of possible adversary behaviors to test or derive a series of findings. Table (6-9) outlines the key attributes and fundamentals of the NWC/ONI red-team development and application approach. It is not all inclusive but builds on respondent and ONI red-team discussion documents.

KEY ATTRIBUTES	FUNDAMENTALS (from Red team Perspective)[136]	METHODOLOGY	MENTIONED BY RESPONDENT
War game definition	Game Definition-- Joint Pub 1: A simulation, by whatever means, of a military operation involving two or more opposing forces, using rules, data, and procedures designed to depict an actual or assumed real life situation.	n/a	Yes
War game definition	McHugh (1966): A simulation of selected aspects of a conflict situation in accordance with predetermined rules, data, and procedures to provide decisionmaking experience or provide decisionmaking information that is applicable to real-world situations.	n/a	Yes
Benefits	The Decision= Heart of the Game Strength-- psychological power, ego involvement, investment & ownership, and consequences.	n/a	No
Benefits	Consensus building, shared experiences, insights— New ways of conceptualizing the problem, new courses of action, new elements of information needed for a decision, previously unknown relationships between aspects of a problem, understanding problem dynamics, motivations of choices.	Process	Yes
Fidelity	Can be an abstraction, distillation, or simulation.	War game type	ONI war-gaming brief
General Purpose	Can be educational or analytical	War game type	ONI war-gaming brief
Number Of Sides	One, two or n	War game type	ONI war-gaming brief
Intelligence/ Information	Can be open or closed	War game type	ONI war-gaming brief
Method Of Evaluation	Can be free, semi-rigid, or rigid	War game type	ONI war-gaming brief
Simulation Technique	Manual or computer aided	War game type	ONI war-gaming brief
Time	Time can be in blocs or segments, mixed, or running --teams have a limited or unlimited amount of time to let battle or engagement run its course—this allows adversary to attempt to get in other's OODA loop and other unforeseen events occur	War game type	ONI war-gaming brief
Scope	Can be echelons, services, or based on geography	War game type	ONI war-gaming brief

Table 6-9: Key NWC/ONI DET War Game Attributes[137]

6.4.2 Office of Naval Intelligence (ONI) Detachment Red-Team Development

From the ONI wargaming perspective, red teams are second only to the blue team in importance and are taken very seriously. The *Adversary Force Perspective* ONI brief from 2009 states that:[138]

> "Red-teaming will not prevent surprises. Surprise is inherent in a world dominated by chance, ambiguity, and uncertainty. But red-teaming can prepare military organizations to deal with surprise. In particular, it can create the mental framework that is prepared for the unexpected and it is the skillful, intelligent adaptation to the actual conditions of war that best leads to victory."

According to McKenna and Fontenot (2005), successful red teams are composed of highly qualified experts in their field; intellectually honest with an uncanny ability to find the holes in the blue team's course of action; with sound reputations and even temperaments; credible, perceptive, and articulate; and have a good understanding of their role and purpose (which is to make the blue team better).[139]

What makes red teams weak is (1) not composed of adequate experts in their field; (2) The team fails to take assignment seriously; (3) they lose their independence and are manipulated by their scenario, environment, or the blue team; (4) they become too far removed from the decision-making process e.g., they are marginalized and/or viewed as just another "side-line critic."[140]

Red teams are also very dependent on what the game objectives are. Game objectives are often defined by:

- What decisions does the sponsor want players to grapple with?
- What activities does sponsor want red and blue teams to participate in?
- What deliverable/evaluation/assessment is ultimately being provided?[141]

Objectives Define:

- Issues To Be Addressed
- Appropriate Scenario Options
- Geographic/Opponent Options
- Structure Of The Game
- Player Cells / Roles / Invitees
- Timeline
- Hidden or additional but not apparent to participants
- Stated With Finesse: Study, Assess, Examine, Gain Insight but never provide absolute certainty or validation of a particular approach (McKenna, 2009).[142]

6.4.3 ONI Detachment Red-Team Process within (NWC War game Development)

A generic process steps matrix for the NWC/ONI Detachment (DET) war games is found below in Table (6-10). It bears little similarity to the US Army UFMCS process matrix because it is a war game development process with red teams as threat

emulation components-- not the UFMCS steps used to create a red team for validating decisionmaking. This key difference is the first of many that will drive a distinction between threat emulation and decision support red teams (see conclusion of the study).

PROCESS STEPS	RATIONALE
1. Sponsor comes to NWC ONI/DET and requests assistance	Funding/resources
2. Center for Naval Warfare (CNW) studies director reviews request--Determines if logistical requirements are met	Can NWC accommodate Request
3. Game director provides opinion (O6-level) to sponsor and NWC provost	Leadership approval
4. Game/study is commissioned	Game is approved
5. Games director (lead contractor or O5) builds a staff to conduct game	Director builds staff to conduct game
6. Staff consists of: 12 person detachment w/2-3 active duty, lead game designer, 2 O5s or GS13-14s, 3-4 other WG junior officers (O3 or O4), 3-4 enlisted men/women), Judge Advocate Group (JAG) for Rules of engagement and legal questions, some subcontractors depending on subject matter	Pre-existing team for game development
7. Phase 2: DC Plan lead	Game planning phase begins
8. Red team needed--call War Game dept. to build action plan	Red Team need identified
9. 45 games a year in various configs are conducted	Throughput
10. so far NWC has conducted 240 games but does not have time or staff for trend analyses, comparisons etc.	Limitations on meta analysis of games
11. Wargaming conference to identify key membership, & Head red team leader	RT defined and planned for—includes arrangement of expertise from outside NWC, subject matter experts from academe, private sector, FFRDCs, etc (not formalized)
12. If greater involvement needed by particular elements are identified, ONI DET arranges or sends requests, Service level agreements (SLAs), etc	If necessary, NWC game director must arrange service level agreements or statements of agreement to obtain SMEs or technological assistance depending on game complexities.
13. Intermediate planning conference to work out particulars (riverine, littoral, diesel electric boat exp.)	Planning conference to work out details including red team issues, challenges, problems with adequate realism as defined by game director and staff.
14. Since 9-11 there has been increase in #s and rigor	Depending on game and RT involved, steps must be taken to ensure adequate realism and rigor or explanation of game limitations.
15. Many civilian professors and retired O5s avail to increase realism	NWC reaches back to obtain experts on complex and/or little understood topics, religious subject, historical issues, culture, etc.
16. Additional move to utilizing more technology and virtualization resulting in increase in connectivity, networking, etc.	New technologies and networks used when applicable to game subject matter.
17. Validate game plan of action and milestones	Game director validates plan and gantt chart of game
18. Review game objective drill-downs, and sub-processes	Game director drills down into subject matter to ensure sub-elements are understood by game participants including red team.
19. SOF plan, AIC planning, grand strategy	Game director determines best way to achieve overall game objective
20. Head red joint staff equivalent unless it's a vignette not a scenario (Vignettes used by National Defense University and others and limit use of red team as defined in study)	Red team staff elements or SMEs derived to put together red team Rules of engagement (ROE)
21. Determine red team ROE, data collection, analysis planning, game design, red team people, SMEs in x,y,z	Red team rules of engagement, etc. are Determined to understand how red team will operate, plan, execute, collect intelligence/analyze, respond to Blue
22. Any intergov , UN, neutral decisionmaking is applied	White team development Determined
23. RFI desk creates *smart* books developed for all teams--containing strategic objectives; Red's desired end state; mull it over and develop questions	Individually team focused notebook-like documents created with all info, ROE, resources, order of battle, objectives, desk guide, etc for each color team
24. Determine green team-neutral other nations; white team-natives other noncombatants; blue team-sponsor or US forces; red team-adversary; pink team-red teams embedded in white; control cell/team adjudicates disputes or questions	Peripheral or other forces, organizations, etc. depending on game complexity/objectives and *smart* books developed for those teams created as well
25. All participants briefed in auditorium re: objectives and who will be doing what--ROE	All teams briefed in large venue to hear same thing (i.e., ROE, time, address other variables)
26. Scenario brief--i.e., "road to crisis" unless it's a vignette depending on sponsors pockets	Scenario may be briefed at this time
27. CNN version--"given where you are right now…" briefing in provided to participants	Each team is told where it is right now –at start of "crisis" e.g., beginning of game
28. Go to your breakout room/cell and blue and red teams receive a tailored to team brief	Each team retires to breakout rooms to receive their smart books and a brief tailored to their team outlining add'l information, admin. Info, time to complete turns requirements and definitions
29. Brief provides high level understanding including misperceptions of other teams--ground truth according to your team's intelligence apparatus	Briefs provide information on other teams (some of which may be based on faulty intelligence or cultural misperceptions)
30. RT determines how it will achieve team's objectives (provided a tailored template)	Team discusses, plans, and documents what it will be doing to achieve its objectives based on available data
31A. Example: five days of back and forth--based on known models and simulations, dice, or BOG set; each move of each team is charted adjusted, assessed, feedback to go its course…	In maximum case, five day scenario—teams take turns back and forth as the game is played out
31B. Max 5 moves proceeded by custom template tailored to sponsor's needs and complexities--to capture outcomes for sponsor	Findings & outcomes are charted, computed, & tabulated to Determine what COA implemented by teams to achieve objective based on what other teams did--
32A. At the end participants reconvene in auditorium for debrief…	Debrief

32B. After action review--receive game report and lessons learned provided to sponsor that is property of sponsor	After Action Review/Lessons Learned (LL)
33. Discussion of obvious stuff objectives , methodologies, etc	Discussion of what went wrong/what was done well
34. Issues and analysis provided	Issues, challenges, analyses provided sponsors
35. Results and recommendations issued	Results collected & documented
36. Need for better Intelligence, surveillance, reconnaissance (ISR), command and control, etc.	Larger domains or disciplines' issues identified
37. Assessment and adjudication sessions	Final adjudication and outputs derived and distributed to sponsors

Table 6-10: Key NWC/ONI DET Red-Team Process Steps[143]

(Red highlights red-team participation in ONI DET war game process)

According to McKenna (2009), game designers at ONI/DET ensure red-team leadership has a role in the game design (step 21). ONI/DET designers also encourage red-team SMEs to assist in developing/reviewing the scenario or war game brief such that it is plausible and consistent with strategic objectives. Additionally, game designers ensure adversary force organization, gaming facilities, deliverables, are accurate, understood and factored into the game planning process. Game designers sponsor opportunities to plan and execute red-team workshops independent and/or ahead of the main event to identify realistic strategic and operational objectives outside blue-team domain issues, challenges, and technologies. McKenna goes on to state that game designers specify desired end states of games and work with red-team SMEs to develop Concept of Operation (CONOPS), plan red-team organization and manning strategies, ensure red Order of Battle (OOB) and capabilities are acceptable and accurate, and decide on initial force orders of battle.[144] Key drivers of NWC war games that were mentioned by respondents and contained in their briefings are listed below in Table (6-11).

These drivers are the tenets and military instructions that the ONI/DET war gamers use to justify their approaches and resolve questions between sponsors and war game organizers and between red and blue teams if issues arise. The games can get very heated as favorite doctrines, weapons systems, and strategies get tested in a laboratory setting. The drivers are much like legal precedent. They will not eliminate conflict but provide a good starting point for conflict resolution. Their clarity is helpful to all participants and their inclusion in red- and blue-team briefing packets is a necessary element.

FUNDAMENTAL TENETS/REQUIREMENTS	WAR GAME RELEVANCE
JOINT PUB 1: A simulation, by whatever means, of a military operation involving two or more opposing forces, using rules, data, and procedures designed to depict an actual or assumed real life situation.	SPONSOR can be--Naval COMPLAN, PACFLT, OPNN, ONI, NMIC, N34, IC, DHS, MIL sealift command, USGovt, NDU, etc
MCHUGH(1966):A simulation of selected aspects of a conflict situation in accordance with predetermined rules, data, and procedures to: Provide decision-making experience, or provide decision-making information that is applicable to real-world situations.	Game designers--experts in Wargaming
PERLA & BARNETT(NWCR,'85): Any type of warfare model or simulation, not involving actual military forces, in which the flow of events is affected by decisions made during the course of those events by "players" representing opposing sides. not: analysis; real; repeatable--exercise in human interaction and the interplay of human decisions and the outcomes of those decisions	Problem to be solved
DENNIS CALLAN: The creation of a moving context within which players are required to make decisions, for the purpose of having a worthwhile conversation and gaining insight on tactical, operational, or strategic issues	Complexity

Table 6-11: Key NWC/ONI DET Red-Team Tenets[145]
(Mentioned by Respondents)

Figure (6-1) below, outlines the one-sided game move cycle for the red and blue teams. Note the simple approach used as the *Control Team* which includes a red component, responds to a blue team first move as it responds to a particular condition.

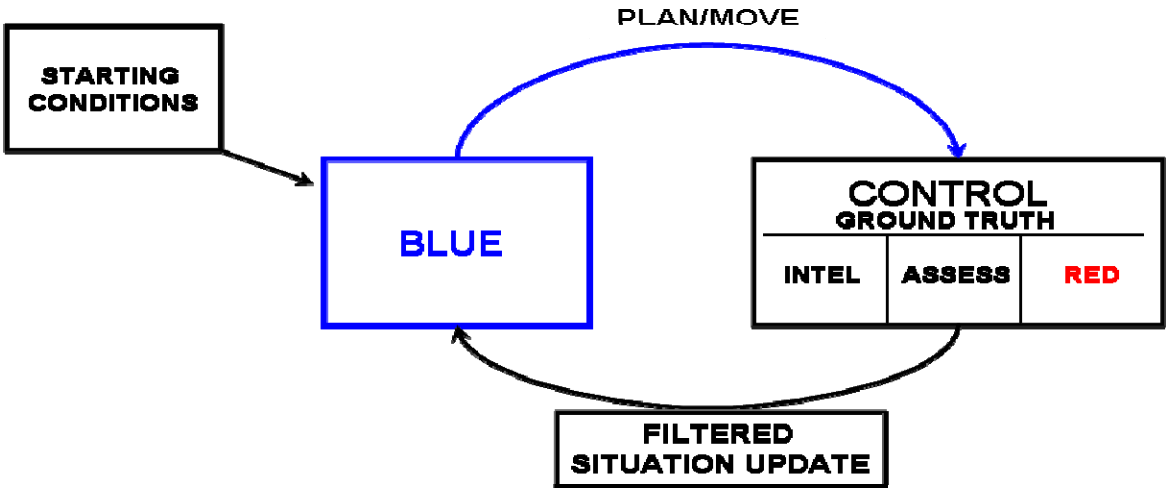


Figure 6-1: One-Sided Game Design
(Used with permission from McKenna, NWC)

For a two-sided game, both red and blue are responding simultaneously to separate starting conditions. Then both red and blue are provided with filtered situation updates based on their predetermined abilities to collect intelligence and assess the "ground truth" (see Figure [6-2] below).

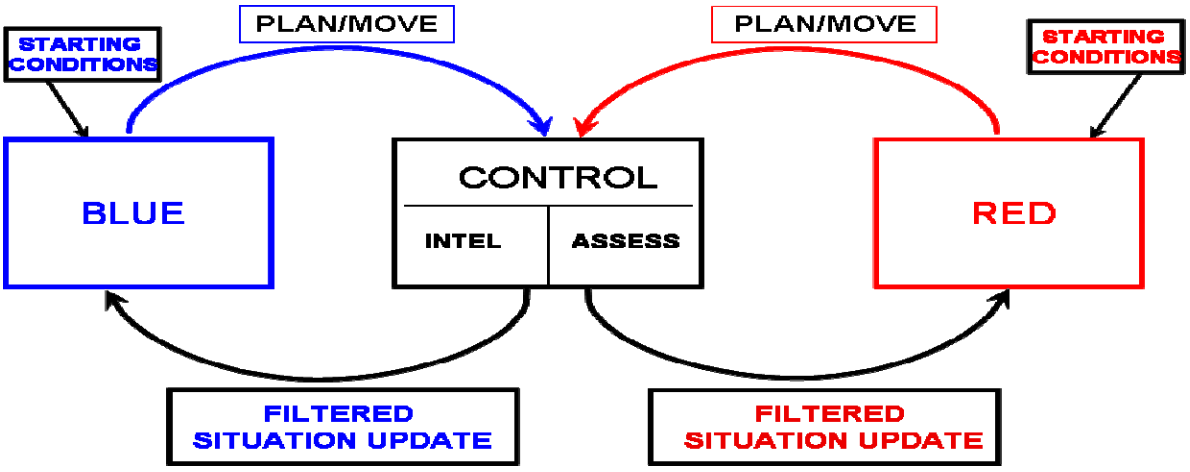


Figure 6-2: Two-Sided Game Design
(Used with permission from McKenna, NWC)

Both blue and red courses of action processes are based on a separate series of decision inputs that lead each team to a course decision. The blue team relies on *friendly* (American or coalition forces) mission/intent, friendly objectives, and friendly capabilities independent of red team. The blue team must identify 2-3 possible courses of action (COAs). While the blue team is determining its COAs, the red team also works through its own determination of enemy capabilities, enemy objectives, and enemy intent independent of blue team. The red team will determine which COA is most likely and dangerous based on its understanding of blue. See Figure (6-3) for a simple explanation of the COA/ECOA development. The Objective of the red cell is not to "win" by defeating friendly COAs, but to assist in the development and testing of friendly COAs.[146]

Friendly Courses of Action (COAs)	Enemy Courses of Action (ECOAs)
•Based on	•Based on
•Friendly Mission / Intent	•Enemy Capabilities
•Friendly Objectives	•Enemy Objectives
•Friendly Capabilities	•Enemy Intent
•3 COA's usually developed and analyzed	•Most Likely & Most Dangerous

Figure 6-3: NWC/ONI DET Blue and Red Courses of Action Comparison

6.4.4 ONI Detachment Red-Team Measures/Metrics

ONI/DET respondents believe that their successful red teams are clear on their ultimate objectives and understand their strategic, operational and tactical objectives before employment. Their actions support attainment of those objectives and build towards a desired end-state which is the collection of data on red –blue engagement. Red-team leaders communicate modes and objectives to the rest of the team and are familiar with their entire Order of Battle (OOB) as well as platform capabilities and limitations. They are also familiar with *assessed* operational capabilities and limitations.[147] For example, an adversary with a submarine that is theoretically capable of firing torpedoes but rarely gets underway, isn't integrated into the red-team war fighting doctrine and hasn't successfully fired a torpedo for 7 yrs is a much different threat than an adversary that can effectively employ the weapon system. Game objectives drive key red-team design parameters (listed below in table [6-12]).

Based on game objectives, the ONI/DET red teams are designed to help discover new thinking, attain consensus in an approach, identify previously unknown relationships between aspects, help prepare or expose a lack of preparation, or assess a series of alternatives. Per the NWC/ONI DET red-team model, the game objective steers game designers towards a given hypothesis in which the red team acts as an independent variable. If the game objective is threat emulation for example, the red team may be designed as the threat and game designers will focus on collecting information on blue response to the threat. For example, for scenario resolution, the red team:

> "The designer of a war game has great power to inform or to manipulate. The players and others involved in the game and its analysis must be aware of this danger. They deserve and should demand an explanation of why events run counter to their expectations. They must be allowed, indeed encouraged, to be wary and skeptical and to question the validity of insights derived from the game until the source of those insights is adequately explained."—Peter Perla (1990)[148]

Unfortunately, the NWC/ONI DET does not run any types of macro or meta-analysis on war-gaming trends or go back and validate findings from old games due to funding and

time constraints. This type of information could be useful in improving games and red teams. Table (6-13) below depicts which types of outputs and findings are desired based on NWC-ONI DET games design parameters and objectives.

GAME OBJECTIVE/ KEY DESIGN PARAMETERS	MANIFESTED BY OUTPUTS SUCH AS:
Threat emulation	New ways of conceptualizing the problem New courses of action New elements of information needed for decision Previously unknown relationships between aspects of a problem Understanding of the problem's dynamics Motivations for choices: made/rejected
Scenario resolution	Refine Concepts, Doctrine, and Issues Build Consensus Test run Plans, Concepts, Technologies Identify Issues, Capabilities, & Deficiencies Permit Risk-Taking Assess Alternatives Replicate Decision-Making Conditions Help Prepare Military Organizations to deal with Surprises
Generate some friction	Motivations for choices: made/rejected Refine Concepts, Doctrine, and Issues Replicate Decision-Making Conditions
see US Navy NWC Proceedings Spring 2006 Wednesday, January 31, 2007 What Can We Learn From War-gaming? "The Epistemology of War-gaming" - This article from the Spring 2006 Naval War College Review addresses the question of how one can assess the knowledge gained from a war game. Can one extract valid knowledge that will be of use in future, while avoiding drawing unsupported conclusions?	

Table 6-12: Key NWC/ONI DET Red-Team Design Parameters[149]

According to McKenna (2009), the NWC/ONI DET red-team approach stresses the following elements in relation to the blue team:[150]

- Know the "enemy" (the blue [American or coalition] team);
- Make an assessment of the blue-team strategic, operational and tactical objectives;
- Identify the blue-team Centers of Gravity and focus on neutralization based on red-team objectives;
- Make an assessment of the blue-team desired end-state;
- Understand results may not be clear at first application but may be worthy of some additional analysis;
- Be familiar with the blue-team entire order of battle (OOB) as well as platform capabilities and limitations;
- Do not focus on just the blue maritime forces;
- Be familiar with the blue-team Operational capabilities and limitations
- Provide a short declaratory statement of the "why" and "what for"

Without follow-on metrics, these claims may or may not always be accurate. There are multiple options available to the war game designer to extract the most out of the interaction between *Red* and *Blue*. As an inexact science, there is much room for error,

although the ONI DET team is well aware of this fact according to respondents. They do caveat their findings and limit conclusions. Table (6-13) below provides the primary exercise or war game types used by ONI DET to capture specific red-team characteristics with time options used to test hypotheses.

ONI EXERCISE/WAR GAME TYPES	RED TEAM CHARACTERISTICS	TIME (Running Clock or Move Convention days/weeks/months)
One Sided Game Design	Advantages Easily Controlled Fewer Players/Controllers Disadvantages Players Perceive Manipulation Inappropriate To Examine Some Issues Deception Insight Into Differential Perception Information Dominance Deterrence Requirement Roadmap	Time: Running Clock Appropriate For Tactical Considerations Inappropriate for Long Temporal Horizon Strategic Considerations Theater Logistics War Termination Extended Deterrence: Seldom Overtakes Player Decisions; But The Higher The Command Echelon, The More Likely To Be Bored
		Time: Move Convention Days/Weeks/Months Seminar Games Appropriate For Extended Temporal Horizon Time Or Event Driven Simultaneous Or Alternating Risks Bypassing Major Decision Points Time Step: Vignette Almost Impervious To Player Decision-making
Two Sided Game Design	Advantages Natural Human Competition Investment More Complex Issues Examined Disadvantages Mechanical Complexity Difficult To Control	Time: Running Clock Appropriate For Tactical Considerations Inappropriate for Long Temporal Horizon Strategic Considerations Theater Logistics War Termination Extended Deterrence: Seldom Overtakes Player Decisions; But The Higher The Command Echelon, The More Likely To Be Bored
		Time: Move Convention Days/Weeks/Months Seminar Games Appropriate For Extended Temporal Horizon Time Or Event Driven Simultaneous Or Alternating Risks Bypassing Major Decision Points Time Step: Vignette Almost Impervious To Player Decision-making
Multi-Sided Games	Geopolitical Vice Warfighting Players = Country/Faction Teams Maximum Of 8 Sides Preferably 6 Too Many Moving Parts	Time: Running Clock Appropriate For Tactical Considerations Inappropriate for Long Temporal Horizon Strategic Considerations Theater Logistics War Termination Extended Deterrence: Seldom Overtakes Player Decisions; But The Higher The Command Echelon, The More Likely To Be Bored
		Time: Move Convention Days/Weeks/Months Seminar Games Appropriate For Extended Temporal Horizon Time Or Event Driven Simultaneous Or Alternating Risks Bypassing Major Decision Points Time Step: Vignette Almost Impervious To Player Decision-making

Table 6-13: Key NWC/ONI DET Red-Team *Conduct Exercise* Process Steps[151]

6.4.5 ONI Detachment Red-Team Challenges and Best Practices

McKenna also emphasized the fact that the ONI DET approach included understanding that the red-team developers must focus on the objectives and purpose of the game. There are times when implementing a certain Enemy Course of Action (ECOA) is desirable to meet game objectives and as long as this artificiality is agreed upon, stated upfront and captured in final reports that are acceptable--if not, the game is prone to failure.[152] The example McKenna sites in his *An Introduction to Wargaming from the Adversary Perspective* (2009): [153]

> In Millennium Challenge 2002, a $250 million war game designed to test the new technologies and concepts of transformation and network-centric warfare—in which U.S. forces are data-linked with one another as never before—Lt. Gen. Paul Van Riper, former president of the Marine Corps University, was asked to command the "enemy" forces. In the first days of that mock battle, he used unconventional methods, including a preemptive attack that featured air-, sea-, and ground-launched cruise missiles to sink 16 American ships. After the American forces decided to refloat the ships and restart the game, Van Riper stepped aside from his role, contending that the rest of the game was scripted for American victory.[154]

Other red-team practices mentioned by McKenna that are important as the ONI/DET red-team moves through its development paces:[155]

- Avoid mirror-imaging the blue-team values, social mores, and cultural attributes:
- Accurately play the adversary force by:
    - "Think Red"
    - Be familiar with Red cultural norms, biases and ethno-centric tendencies
    - Be familiar with Red Rules of Engagement (ROE)
    - Be familiar with Red decision-making apparatus
    - Be familiar with Red doctrine and tactics
    - Beware of excessive rigidity
    - Balance methodological steps with "free-play/exploration"
- Planning is critical:
    - The red team must develop a well-thought out red-team planning process prior to engagement;
- Avoid having the red (team) operating in an unorganized fashion (this is not educational nor is it realistic);
- Understanding how and why the adversary force employs their force is often the most critical element of learning and is one of the most difficult to interpret

Upon completion of the wargaming exercise, and from an analytical stand-point, there is a distillation of findings, outputs, and/or results if the game designers were successful. Table (6-14) below illustrates probable findings from ONI DET wargaming exercises and compares results with critical questions and some challenges associated with the results.

COLLECT FINDINGS/OUTPUTS	CRITICAL QUESTIONS	CHALLENGES
New ways of conceptualizing the problem	Were Geopolitical Events Up To Start Of Decision Process correct?	COMMON PROBLEMS: --Indications and Warning (I&W) and Flexible Deterrent Options (FDOs) (e.g., did blue team miss queue/been asleep at the switch?; --Ignoring the obvious—or ignoring possible courses-of-action due to heat of battle; --If Hostilities occur, what's Happened?—communications may be overly limited. Red or blue or other noncombatant teams may not know what is occurring;
New courses of action based on problem set	Are these items dependent or independent variables? • Geography • Command Echelons • Red/Blue • NCA • Services • Other Actors: • State Dept; NGO/PVO; Allies • Defined By Game Objectives	
New elements of information needed for decision	Rigid Systematic Models/Lookup Tables Free Expert Opinion Best Military Judgment Semi-rigid Mixed	
Previously unknown relationships between aspects of a problem	Was this relationship adequately accounted for? Is my data correct?	
Understanding of the problem's dynamics	Are there complexities we were not aware of?	
Motivations for choices: made/rejected	Are motivations adequately captured to discern this?	
New ways of conceptualizing the problem	Is this an actual new problem?	
New courses of action	Does this new COA require new training, doctrine changes, new systems?	
New elements of information needed for decision	Do we currently collect this level of information or is a new collection system required?	
Refine Concepts, Doctrine, and Issues	Will refining concepts, et al change outcomes?	
Build Consensus	Is there groupthink?	
Test run Plans, Concepts, Technologies	Can we do this?	
Identify Issues, Capabilities, & Deficiencies	Correctly identified?	
Permit Risk-Taking	Does this level of risk taking go against culture and/or doctrine?	
Assess Alternatives	All relevant alternatives accessed?	
Replicate Decision-Making Conditions	Can experiment be repeated with same results?	
Help Prepare Military Organizations to deal with Surprises	Are we relevant?	
Successes: policy changes	Are all policy changes identified?	
predictive gains/correct	Is explanation correct? (type II errors)	
Explain what happened	All technical surprise identified?	
Avoid technical surprises	Planning decisions really improved based on findings?	
Significant planning decisions impacted		
Scenario Considerations		
Scope of a Game		
Do not do very much with non state actors—they are difficult to war game	Non state actors ignored?—YES currently unable to simulate(!)	

Table 6-14: Key NWC/ONI DET Red-Team Findings *Collection Process* Steps[156]

6.4.6 Final Thoughts and Relation to the DoD/Military Red-Team Model

Many threat emulation or *standard* wargaming methods are used by ONI DET to accomplish its mission. Unlike UFMCS, ONI DET focuses on more laboratory

experiments of interesting scenarios to *draw out conclusions* whereby UFMCS is *building* a cadre of red thinkers. ONI DET primarily investigates the Action -- Reaction -- Counteraction methodology that examines specific critical events between red and blue forces. The result of this interaction is ONI DET's essence for being. Whereas ONI DET's red teams are validating or improving blue systems and doctrine, UFMCS uses as many methodologies as digestible by the student red-teamer to expand the ability of its charges to identify weaknesses and then coherently articulate shortcomings of corps, divisional, and brigade/battalion level planning. Both organizations grapple with inserting new nonlinear thinking as much as possible but they are both tied to the DoD/Military rational approach red-team model. The UFMCS red-team objective is to improve blue thinking processes. ONI/DET provides classic or traditional red teams in the U.S. Air Force Red Franchise model outlined by Malone and Schaupp whereby the ultimate objective is to improve blue-team decisionmaking and possibly identify doctrinal or training shortcomings not apply non-linear or unconventional non-state combatant weapons, tactics, devices to traditional military force structures.

6.5 Combatant Command X Red Team

6.5.1 Defense Intelligence Operations Coordination Center (DIOCC) Concept

The Secretary of Defense and the Chairman of the Joint Chiefs of Staff have authorized a number of mechanisms to strengthen and better promote collaboration between and among Combatant Commands (COCOMs), defense intelligence establishments, and other civilian agencies such as the Department of State, Homeland Security, and Department of Justice.

Two such mechanisms that utilize red teams are the focus of this section. One is the establishment of the Defense Intelligence Operations Coordination Center (DIOCC). The other is the insertion of formally trained red-team leaders (RTLs) and red-team members into the COCOM planning process itself. The DIOCC is intended to

strengthen the ability of defense intelligence to synchronize intelligence operations and collection to support the Combatant Commands and provide a vehicle to better insert alternative thinking into understanding possible adversaries. A few COCOMs have been able to stand up red cells to provide their commanders with alternative analysis and post red–team analytical products and tools on the Secret Internet Protocol Routing Network (SIPRNET) classified network and other networks for dissemination to other commands and government entities with proper accesses.

The DIOCC integrates into a single organization the functions of the Defense Intelligence Agency (DIA's) Defense Joint Intelligence Operations Center (DJIOC) and the United States Strategic Command's Joint Functional Component Command for Intelligence, Surveillance and Reconnaissance (JFCC-ISR). The DIOCC also serves as the Defense Department's focal point to interface with other newly established intelligence centers such as the National Intelligence Coordination Center (NIC-C) and the National Counterterrorism Center (NCTC).

The other key mechanism of the DIOCC and its parent organization DIA, is the partnering with UFMCS and the advanced Service schools such as NWC, Air Command and Staff College, and the Army Command and General Staff College to develop red-teamers to embed in the J-2 (Intelligence) organizational unit within Combatant Commands, Corps-level and other DoD intelligence centers such as the National Ground Intelligence center (NGIC) supporting the Army, the National Aviation and Space Intelligence Center (NASIC) supporting the Air Force, the Office of Naval Intelligence (ONI) supporting the Navy, and the Marine Corps Intelligence Activity (MCIA) supporting the Marines. The DIOCC also receives UFMCS graduates and acts as an operations and intelligence hub for DIA that coordinates DIA-COCOM activities around the globe and allows commanders to quickly reach back for DIA resources, expertise, and other government coordination operating in a 24/7 capacity.

6.5.2 Joint Intelligence Operations Center (JIOC) Concept

In 2006, the Secretary of Defense, through the Joint Chiefs of Staff, directed the combatant commanders (COCOMS) to establish Joint Intelligence Operations Centers (JIOCs) for conducting intelligence operations in support of DoD operations worldwide. This direction is based on the Taking Stock of Defense Intelligence (TSDI) study and the Remodeling Defense Intelligence (RDI) Implementation Strategy document. JIOCs are, in part, a result of the RDI recommendations to "strengthen COCOM ability to conduct a range of intelligence operations making use of appropriate source or method and with access to all relevant data or information." Furthermore, the JIOC Execute Order (EXORD) states that "each JIOC shall routinely employ red teams to address the commanders' most pressing intelligence and operational issues from alternative perspectives, to include assumptions, second-order effects, intended outcomes and information operations through anticipated adversaries' perspectives."[157]

When embedded in intelligence-focused organizations such as JIOCs, red teams are intended to improve intelligence estimates and plans. Red teams embedded within the JIOCs help the staff define how cultural perspectives shape enemy goals and objectives. Additionally, these red teams are intended to assist the command staff in understanding and accounting for variables found in the operational environment impacting enemy courses of action, and in identifying disconnects in the intelligence portion of plans to better synchronize supporting/supported intelligence operations. The reality is many COCOMs do not yet have such functional entities.

It is within this proposed new environment that the Combatant Commands are also instituting a number of new red-team initiatives. The initiative that this chapter on COCOM red-teaming illustrates, is the embedding of red cells into COCOMs based on USD(I) policy. The section on UFMCS discussed sending out trained RTLs and red-team members to operational elements. In addition to the DIOCC, the COCOMs are operational elements that have been receiving these red-teamers as well. Not all COCOMs have accepted or are able to immediately train and provide red-team space,

connectivity, and integration into COCOM planning and operations. The following is a case study of one COCOM that has embraced the concept of red teams and has accepted graduates of UFMCS and has provided a proof of concept for reach back to the DIOCC to sustain its functional red team.

6.5.3 Case Study: COCOM X Red-Team JIOC

In this case study, one of the United States' oldest combatant commands, *COCOM X* [1] has been a force for stability and a committed partner in its Area of Responsibility (AOR) for more than 60 years. With an AOR that includes more than 3 billion people and encompasses about half the earth's surface, the Command remains a significant stabilizing influence in the world. The Command is very proud of its legacy and plans on enhancing its substantial engagement with national and international partners in preserving the security and stability upon which the region's success depends. Among *COCOM X*'s AOR and the foreign leaders therein, *COCOM X*'s commander and joint staff believes there is an understanding of the enormous potential for progress through existing relationships and the advancement of shared security goals. [158]

The Command and its staff recognize the complexity of its security environment and the importance of proactively employing forces in ways that strengthen partnerships and support conditions that preclude the necessity for combat operations. This strategy underwrites the National Defense Strategy by linking *COCOM X's* activities and operations to U.S. Government policy and strategic guidance. It illustrates the realities of the dynamic region, presents Command imperatives, and defines its objectives. The Command will operationalize this strategy through its Theater Campaign Plan which shapes its contributions toward a secure, stable and prosperous AOR.[159]

[1] COCOM X is not identified in this study due to classification concerns in connecting a geographical location to the use of red teams in that area of responsibility.

6.5.4 Linking the JIOC Red Team to the COCOM Joint Intelligence Planning Process

One of the key areas within COCOM *X* planning the DIOCC/JIOC red teams are attempting to be an integral part of concept development and planning, is contributing to the Joint Intelligence Planning of the Operational Environment (JIPOE) process. This process identifies potential adversary Courses of Action (COAs); assessing which adversary COA is most likely and which COA is the most dangerous to mission accomplishment. During COA analysis, each friendly COA is gamed against the adversary COAs identified through the JIPOE process. The combatant command J-2 and JIOC analyze and evaluate the advantages and disadvantages of each friendly COA from an intelligence perspective and, in conjunction with other combatant command staff elements, provide a recommendation regarding the friendly COA with the highest probability of success.[160] This is a concrete example of an area respondents believed their red teams can help the COCOM *X* planning process.

Red teams provide the Joint Force Commander (JFC) and the Defense Intelligence Operations Coordination Center (DIOCC) Director with an independent view of alternatives in operational concepts, organizational constructs, planning assumptions, cascading effects of Blue actions, and assessments from the perspectives of adversaries, partners and others to improve decisionmaking and planning. They conduct alternative analyses that recognize and evaluate the impact of various cultural and environmental variables. They also review plans to identify gaps, vulnerabilities, strategic opportunities and faulty assumptions. The red-team *COCOM X* has instituted is one of the first among COCOMs. It is championed by a dynamic and forward thinking J-2 (intelligence) Vice Admiral who is a red-team proponent and is highly respected within the intelligence and greater DOD communities. This has helped the Command get the red-team resources and contracts in place before other Commands. Additionally, this proponent has taken advantage of his COCOM's vast responsibilities and evolving demands to demonstrate and prove the concept of red teams embedded in Commands.

6.5.5 DIOCC/JIOC COCOM Red-Team Fundamental/Guiding Principles

With the current environment of extreme funding constraints, new initiatives such as building a cadre of red-teamers and applying red teams to combatant command decisionmaking have to show their value within one or two fiscal years or risk being cut. The red-team champion in *COCOM X* has been able to protect the command red team elements within the JIOC and market its products across the intelligence community via for a, symposia, and the SIPRNET. Table (6-15) below, identifies the key attributes of *COCOM X* red cell as designated by the DIOCC/JIOC concept of operations. The DIOCC red team is authorized by Joint Chiefs of Staff Executive Order (JCS JIOC EXORD) 031640Z Apr 06 and JCS DIOCC EXORD 042130Z Dec 07. The operation of the DIOCC red team is specifically addressed in Defense guidance which set up the JIOC:[161]

> Develop national-level defense intelligence support plans for Combatant Command plans and operations, and for defense-level decisionmakers.[162]

The key drivers and attributes of the DIOCC/JIOC red-team model are based on guidance from the Director of National Intelligence (DNI), DIA, and joint DoD publications that outline the goals and objectives of the teams. The fundamental concept of operations and key characteristics are also linked to the guidance documentation below to show the reader what value added the DIOCC/JIOC red team is designed to bring to the commander. Finally, the last column shows whether or not the DIOCC/JIOC respondents and briefing materials mentioned the attribute, fundamental, or characteristic during the study data collection phase.

DIOCC/JIOC KEY ATTRIBUTES/DRIVERS	FUNDAMENTALS	CHARACTERISTICS	MENTIONED BY RESPOND. OR FOUND IN DOCUMENT
Red teams are organizational elements comprised of trained, educated, and practiced experts that provide an independent capability to fully explore alternatives in plans and operations in the context of the operational environment -JP 2-0, 22 June 2007	Each JIOC shall routinely employ red teams to address the Commander's most pressing intelligence and operations issues from alternative perspectives, to include assumptions, 2nd order effects, intended outcomes and information operations through anticipated and adversaries' perspective. ~JIOC Execute Order, April 2006	Any such organs, the creation of which we encourage, must do more than just "alternative analysis, through. The Community should institute a formal system for competitive—and even explicitly contrarian—analysis.…"–Robb-Silberman WMD Report, 2005	Yes
"Red cells" are an important element of war-gaming and are…"A robust cell that can aggressively pursue the adversary's point of view when considering adversary counteraction [to friendly actions]."-Joint Pub 5-0	Conduct alternative perspectives, to include assumptions, second-order effects, intended outcomes, and information operations through anticipated adversaries' perspective."–JIOC EXORD	"The red team is a group of subject matter experts (SMEs) of various appropriate disciplinary backgrounds who provide an independent peer review of plans and processes; act as the adversary's advocate; and knowledgeably role-play the adversary, using a controlled, realistic, interactive process during operations planning, training, and exercising."–Department of Homeland Security	Yes
Joint Publication 5-0, Doctrine for Planning Joint Operations augmented by other service doctrinal and other planning publications provide the Details of how to plan military operations during deliberate (evolving to Adaptive) planning-- "The widely recognized need for alternative analysis drives many to propose organizational solutions, such as "red teams"...	Red teaming is a function executed by trained, educated, and practiced team members that provides commanders an independent capability to fully explore alternatives in plans, operations, concepts, organizations and capabilities in the context of the operational environment and from the perspectives of partners, adversaries, and others. U.S. Army's University of Foreign Military and Cultural Studies*	"Red team Analysis –Models the behavior of an individual or group by trying to replicate how an adversary would think about an issue. …Whereas analysts usually operate as 'observers' of a foreign adversary, the Red team technique transforms the analyst into an 'actor' operating within the adversary's culture and political milieu. This form of 'role playing 'is useful when trying to replicate the mind-set of authoritarian leaders, terrorist cells, or other non-Western groups that operate under very different codes of behavior or motivations."-CIA, Kent Center for Analytic Tradecraft, 2005.	Yes
"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 risk and increase its opportunities….Red teams are established by an enterprise to challenge aspects of that very enterprise's plans, programs, assumptions, etc." Defense Science Board	"The Director of National Intelligence shall establish a process and …ensure that, as appropriate, elements of the intelligence community conduct alternative analysis (commonly referred to as ''red team analysis'') of the information and conclusions in intelligence products."–Intelligence Reform and Terrorism Prevention Act, 2004	" The use of 'red teams' is critical to the ability of commanders and their staffs to understand the adversary and visualize the relevant aspects of the operational environment. ...assist planning by validating assumptions abou Joint Publication 2-0, Joint Intelligence, 22 June 2007	Yes

Table 6-15: Key DIOCC/JIOC Red-Team Attributes[163]

Like a COCOM J-2 (intelligence) commander with JIOC, the DIOCC Director or director designee identifies a red-team staffing solution in accordance with the scope and tempo of red-team activities within the DIOCC. Some combination of full-time, additional duty, or ad-hoc manning likely are required to create teams with changing capabilities while preserving core analytic, critical thinking and facilitation skills.[164] According to Defense Intelligence Agency (DIA) respondents, the practices and attributes listed below are strong contributors to red-team success: [165]

- A red team is able to be heard – its analytic capabilities are understood and embraced by the authority and key organizational players;

• A red team is timely – integrated early into planning efforts to contribute effectively in initial stages of decision-making;

•A red team is relevant – provides information addressing the pressing questions of the commander/director and staff;

•A red team is insightful – demonstrates a deep and applied understanding of the adversaries' and others' cultures, perceptions, motivations, objectives and human factors;

•A red team is agile – not encumbered by recurring production requirements;

•A red team is diverse in expertise and experience – leveraging the skills of trained, educated, critical and creative thinkers both inside and outside the intelligence and defense communities;

•A red team is impartial – possesses great courage and integrity, and is not vested in methods, processes, organizations, outcomes or what is being examined.

These objectives sound impressive, but there are limited mechanisms in the JIOC or DIOCC to build, maintain, or ensure they are true. Funding limitations have limited the metrics that are available so far. Figure (6-4) below depicts the operating environment of the COCOM planning process and where the DIOCC/JIOC red-team construct fits in the DIA. The red-team tools, techniques, and procedures (TTP) are listed in Table (6-20). This red-team construct is a multi-disciplinary approach that seeks to leverage military theory, current events, operational environmental factors, and anthropological factors to distill applications of alternative perspectives especially of country case studies. The benefit is to get American military planners out of cultural attributes and thinking such as mirror imaging, views of the "other", and cultural transference because DIA has identified these attributes as very detrimental to realistically challenging the blue team. This detriment is evident in recent operations in Iraq and Afghanistan operations.

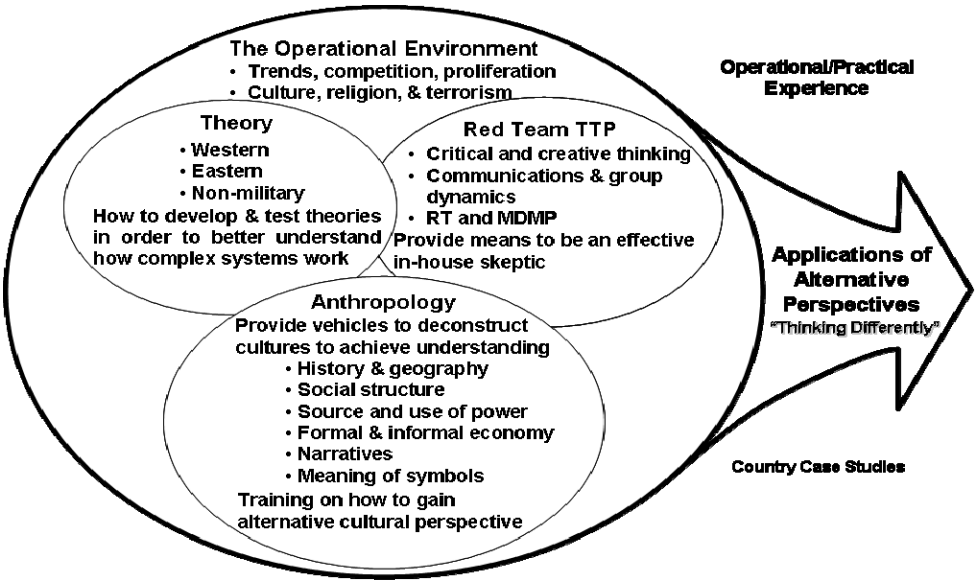


Figure 6-4: DIOCC/JIOC Red-Team Environment

Because expectations of a red team vary widely, it is important to delineate what tasks the DIOCC red team does NOT perform: [166]

> •Penetrate computer systems, communications capabilities or information technologies or identify friendly technical vulnerabilities;
>
> •Conduct quantifiable measures of effectiveness assessments (while the red team may contribute insight to assist in determining appropriate metrics, the process and assessments are inherently U.S., or *blue*, thinking);
>
> •Duplicate existing DIOCC or JIOC red-team responsibilities: the DIOCC red team provides an alternative perspective and contributes to DIOCC functionality, not undermine its expertise. Similarly, the DIOCC red team assumes a support role when working with COCOMS; it is additive and not duplicative.

According to the red-team Concept of Operations (CONOPs) as outlined by Kibiloski (2009), the DIOCC Director will establish an organizational and process structure for Red-team activities to accomplish objectives and realize desired effects. The following is a notional list of DIOCC roles and responsibilities:

> **Red Team Leader (RTL):** The DIOCC Director appoints a full-time, permanent RTL with appropriate leadership skills, experience, and knowledge to lead red-team activities. The RTL is responsible for all aspects of red-team operations and ensures that the results of the red-team's analyses have been properly

conveyed. RTLs should be delegated authority for coordinating and directing red team-related missions. Ideally, the RTL should have a direct line of communication to the DIOCC director or designee, in order to mitigate outside influences on the red team.

Permanent Red-Team Members: The DIOCC will appoint additional full-time, permanent red team members, of whom one may serve as the deputy red team Leader, responsible for fulfilling the roles and responsibilities of the RTL in his/her absence. Permanent members may be any combination of qualified military personnel, government civilians, or contractors.

Ad Hoc Red-Team Members: Additional personnel may supplement the permanent Defense JIOC red team as situations dictate and at the discretion of the RTL. Ad hoc members may include, but are not limited to, personnel within the DIOCC, COCOMs, the DoD, other elements of government, non-governmental organizations, academia or the private sector. Additionally, the red team may establish policies, procedures and tools for facilitating multinational participation in red-team activities. Proper consideration must be given to Director's guidance, security concerns, and operational security (OPSEC) requirements.[167]

Similarly, the *COCOM X* red-team cell consists of an RTL/Director – a retired Navy intelligence officer, with AOR expertise; a deputy RTL with AOR expertise, weapons of mass destruction/proliferation expert, and a master's degree in Public Administration or National Security Policy; two additional permanent red-team members, one with counterterrorism experience and a master's degree in International Affairs; the second, a contractor from an AOR-focused think tank with a broad a social network across the intelligence community and an existing AOR background. Ad hoc members are added depending on J-2 requirements and depending on project's subject, scope and product, augmented by:

- Relevant expert contractors, to advise and/or participate
- JIOC analysts
- J-3 (Operations), J-5 (Planning), component staff officers
- Subject matter experts from the Intelligence Community (IC), academia, private industry
- Collaboration with or support from other Combatant Command Red teams.[168]

Deliverables include regular written alternative assessments, briefings, inputs to working groups, critical reviews and other projects as directed by J-2. They may also include consultation, substantive input, feedback, and written products from contractors.
This structure was mentioned by respondents and by KIbilowski (2009) as providing a dynamic, diverse, and expert in both red-teaming process and substance. Respondents including Kibilowski (2009) also mentioned the red-team organizational structure was balanced between *COCOM X* and non-*COCOM X* perspectives while supporting JIOC mission to collaborate with J-3/J-5 and national agencies[169] Figure (6-5) depicts a notional red-team organization and its relationships within the larger COCOM J-2 structure.[170]

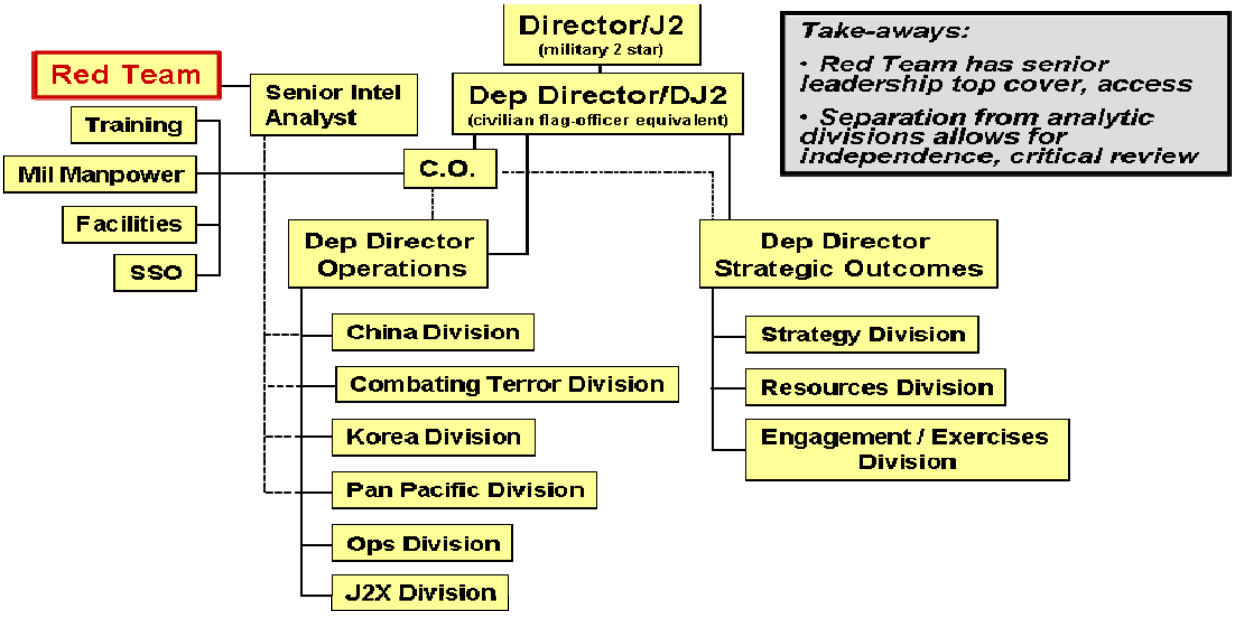


Figure 6-5: Notional Red Team Embedded in COCOM Organization[171]

The Illustration was provided by DIOCC/JIOC respondent; it appears to be a proposal with J-2 as a two star (Vice Admiral lower half) whereby the text notes that currently COCOM J-2 is a three star (Vice Admiral upper half)

6.5.6 DIOCC/JIOC Process Steps

Table (6-16) below depicts a COCOM JIOC red-team process steps taken from Cordray (2007) a COCOM collaborative analytic red-team brief presented to the DIOCC, from interviews with a COCOM *X* JIOC respondent, and from DIOCC respondent.

DIOCC/JIOC RED TEAM PROCESS STEPS[172]	RATIONALE
Cover Administrative Issues –Discuss classification, time available, purpose, process, scope and the desired end state of the session	Take care of matters that could impact work later
Set the Scope –Establish the time frame, area of interest, and other boundaries or limitations based on the overall purpose of the assessment	Determine goals, objectives, relating to AOR in case of JIOC; other intelligence activities in case of DIOCC
Clarify Roles –Participants should clarify their area of expertise or other roles	Determine what each individual brings to team
Establish Ground Rules –Agree upon group norms that encourage a courteous, candid and insightful exchange of ideas while preventing excessive attention given to “pet topics."	In accordance with mission of red team as support function to Intelligence J-2 and Operations J-5
Review key attributes and effects of the operational environment –Examine characteristics of terrain and weather; strengths and vulnerabilities of infrastructures; capabilities and posture of blue forces; and influences of other entities	Ensure team has similar understanding of constraints and assumptions
Review known threat factors–Brief major findings of relevant threat assessments –Brief relevant human factors, if known	Discuss opposing political, economic, military, and psychological characteristics of entities
Identify entities of interest. –Who are the adversaries most likely to take action?	Focus on 2-3 or 4-5 entities that possibly could interest or enter into COCOM planning
What are their most likely capabilities within the operating environment?	Determine what capabilities adversary possesses and are they of interest
What other unique characteristics do they possess?	Does adversary possess other capabilities (such as Chemical, Biological, Radiological, Nuclear (CBRN) or is developing
How do they envision mission accomplishment or success? –Who else may influence or affect the friendly mission? What are their attributes, perspectives, likely actions, etc?	How does adversary define success?
Use the findings to build models and guiding assumptions.	Develop initial models for collective review
Use structured idea generation to postulate WHAT could take place. –How can the adversary capitalize on his capabilities to achieve success? –How can historical analogous scenarios aid the adversary or this red team analysis? –What current terrorism or crime trends illuminate new adversary techniques? –What simple, counter defensive techniques might be used to overcome friendly security measures? –How might other entities affect the scenarios?	SMEs hot wash models to refine or throw out unrealistic assumptions/constraints
Assess which scenarios are most likely. –What cultural, social, or ideological factors might influence the adversary’s preference of one scenario over another? –Discuss Operational Viability –How might the adversary’s view of the operational environment influence their adoption of a particular scenario? –Narrow and rate top scenarios, guarding against “blue teaming” or mirror imaging	Rank order or match models against criteria to Determine likelihood/viability
Determine how a scenario might occur. –What steps will the adversary take leading up to execution of an action? –How will the adversary overcome challenges in the operational environment to achieve successful execution of the COA? –What is a viable tactical plan for the scenario including number of operatives, roles, tactics, weapons, plan synchronization/timing, and contingencies? –What elements of the adversary plan might be observable and indicate that a scenario is imminent?	Back into scenario building based on high probability adversary models
Red team Back brief	Develop draft red team brief or white paper for SME review
Assessment Production	Refine assessment based on edits from red team SMEs and initiate adversary assessment
Assessment Coordination	Coordinate assessment to larger group of military experts around community
Publication and Dissemination	Provide hard copies, soft copies, and post on classified networks on websites

Table 6-16: Key DIOCC/JIOC Red-Team Process Steps[173]

The DIA conducted a red-team survey back in 2008. The findings signified a program still in its infancy with about 60 percent of the COCOMs possessing an actual red team. The DIOCC/JIOC red-team model is seeking to employ its red teams to analyze the most pressing intelligence and operational issues from alternative perspectives. However, with most Command red teams existing less than three years at the time of

this study, it is not surprising that a majority of RTLs come with limited experience and their staffs have even less.[174] As six of the 10 COCOMs have implemented formal red teams with two other commands either activating teams or exploring their role within planning, intelligence, or operational venues. Two-thirds of existing team leaders are full-time.[175] Clearly there is some delay or lack of enthusiasm on the part of some COCOMs in adopting red teams into their command elements. It is unclear whether there is a culture, resource, time, or some other concern that is limiting implementation. More study is necessary to better understand why some COCOMs still do not appear to have red teams in place. The factors holding up the lack of long term assessment of red-team lessons/impacts is critical in better understanding red-team metrics.

The survey also found DIOCC/JIOC red teams are primarily utilized for planning, exercises, and analysis of emerging issues. Although some red teams are augmenting existing planning efforts with non-red team personnel. According to the survey, the majority of time is spent on identifying alternative perspectives among these efforts. Most study areas are self-initiated; other requirements originate from primarily the J-2 and the combatant commander.[176]

The survey also ranked 14 knowledge, skills, and abilities (KSAs) into four general categories based on the number of "votes" they received as follows:

Most Important	**Least Important**
Critical Thinking	Joint Strategic Planning System
Analytical Methodologies	Scenario Writing
Cultures	Team Building
Regional Histories	Anthropology
Asymmetric Warfare	Negotiating
Religions	Professional Writing
Briefing Techniques	Strategic/Operational Theories[177]

The survey found accessing external sources varied among teams. Despite three teams using non-government Subject Matter Experts (SME), generally one third of all SME efforts rely on traditional U.S. Government intelligence analysts. However, teams generally use the Internet, books, or periodicals for offering an alternative perspective

from the intelligence analysts' points of view.[178] The survey also found that depending on experience level, some red teams do not fully grasp how adversaries view blue capabilities (e.g., U.S. force structure, doctrine, allied capabilities in time of crises). Some red teams had no mechanisms to allow them to coordinate their questions, assumptions, constraints, findings with command J-3 operations or J-5 planning elements. Other red teams were hampered by small size of their team (4 people).[179]

Interoperability is essential in establishing a red-team community because bringing together geographically- and mission-dispersed red-team perspectives into a single multi-disciplinary field such as red-teaming, allows cross breeding of ideas, tools, and techniques. A single community implies collaboration between branches of this expertise thereby enhancing the overall red-team community. That is a primary goal of the DIOCC survey and the ultimate purpose of this study.

Most COCOM teams support interoperability by rotating red-team personnel, by developing governance such as a JIOC-wide Concept of Operations (CONOPs), sponsoring an annual conference, and supporting SIPRNET and Joint Worldwide Intelligence Communications System (JWICS) red-team *Intellipedia* web sites. [180]

Table (6-17) below shows the key drivers and rationales for the DIOCC/JIOC red-team approach based on interviews, briefings, and discussions with COCOM and DIA red-team subject matter experts. It is similar to the UFMCS drivers because many UFMCS graduates are being placed in COCOM JIOCs due to the USD(I) guidance referenced earlier in Section 6.

DRIVERS/GUIDING PRINCIPLES	RATIONALE
Guiding Doctrine/References –CIA Kent Center Structured Analytic Techniques –Joint Staff Publication 2-0, Joint Intelligence Driving Factors –Vague Nature of CONUS Threat Reporting –Commander's Requirement for "So What?" –J3 and J5 Requirements for Viable, Realistic Threat Scenarios to Support Planning	Recommended by various executive and legislative commissions: Defense Science Board 9/11 Report Robb-Silberman Report on Weapons of Mass Destruction Homeland Security Institute Required in the intelligence community by legislation: Intelligence Reform and Terrorism Prevention Act, 2004
Red team Analysis is an analytic method, employed by individual analysts and collaborative teams, which models an individual or group to replicate how they would think about an issue, or what actions they may take, given net effects of the operational environment.	JIOC-N Definition of Red teaming "Each JIOC shall routinely employ Red teams(See Joint Pub 5-0) to address the Commanders' most pressing intelligence and operational issues
Structured Brainstorming –A facilitated, focused approach that adheres to ground rules and often employs visual aids or other idea stimulating material. "What If" Analysis –Takes as a given that an event has occurred, then 'think backwards 'to how it could have come about. Structured Analogies –Systematically identifies and rates analogous situations to forecast future problems and discover the most possible outcomes of a given situation. Extreme Users –A method by which a variety of participants are selected based on their expertise, or lack thereof, on the subject being discussed –"inside the box", "outside the box", and "unaware of the box "thinkers. Human Factors–A method by which psychological, ethnographic, or cultural profiles are used. Entity Mirroring –A method by which the analytic team is selected by their similarity of the modeled entity; such as hiring members of the adversary team or individuals with adversary skills or insider, first-hand knowledge. Cultural Immersion –A method by which participants experience stimulus material designed to produce a degree of paradigm shift and inculcate a greater understanding of the adversary's perspective.	Analytical tools promoted by UFMCS training and other red team advocates
Red team goal go against accepted standards, practices, methods, assemble cell, Think Tank & Area studies research, IC, Service, jointly trained personnel, Gain foothold with Commanders, Highly intelligent, No language skills, Military History, send folks to training, Masters in Intl relations, Masters Intl Security, chemistry/cohesive team, fence yourselves off from day to day ops	Analytical tools promoted by UFMCS training and other red team advocates
DoD, USD(I), JCS, COCOM, J-2 leadership must appreciate/understand role of red team provide champion	Concept of proponent or advocacy in ranks
Annual red team conferences, wikis, blogs, and red team support; Staff assistance visits; Connect Subject Matter Experts to COCOM and DIOCC high priority problems; leadership must appreciate/understand role of red team	Support mechanisms
Annual red team international conference held, International participation(i.e., UK, Dutch, AUS, Romanians)	International visibility, support, vitality of discipline
Creation of buzz around red team construct; have success in identifying or correctly predicting adversary behaviors; gain foothold with Blue Team Commanders	Codify JIOC Enterprise Red team Mission in Appropriate Documents
Create and sustain JIOC red team-related education and training venues/curriculum continue to send staff to UFMCS training; create and sustain a culture of collaboration throughout the JIOC Enterprise Red team	Create cadre of experts
Advocate the JIOC Enterprise Red team Mission	Brief approach and RT success to others outside direct community

Table 6-17: Key DIOCC/JIOC Red-Team Drivers/Requirements[181]

The JIOC red teams are funded out of the COCOM's own budget. The DIOCC Office for Strategy and Assessments is responsible for resourcing the DIOCC red team. The red-team leaders (RTL) are responsible for sourcing non-intelligence and/or non-DoD participants to support the red-team mission. The RTL is also responsible for establishing, maintaining and overseeing a permanent red-team capability within the DIOCC. The JIOC red-team composition is more at the discretion of the J-2 commander. This includes staffing of permanent red-team member positions, ensuring

adequate resources exist to train and support red-team members, acquire appropriate tools, and solicit/gain services from subject matter experts as required.[182] Table (6-18) shows the difference between the standard JIOC analysis done for the COCOM and the JIOC red-team approach.[183]

TYPICAL/STANDARD Intelligence Operations ANALYSIS:	JIOC RED TEAM ANALYSIS:
Authoritative	Thought-provoking
Based on evidence (intel reports)	Based on hypotheses
Corroborated and vetted	Not substantiated or vetted
Primarily focused on what Red can do (capabilities)	Primarily focused on what Red and Green thinks (intentions)
Reporting on the operational environment	Thinking about how Blue is – and can – shape the operational environment
Not recommending actions for Blue	Based on understanding Red and Blue and how they affect one another, can consider/propose Blue COAs
JIOC Analysis is: Authoritative Based on evidence (intel reports)	Red team Analysis is: Thought-provoking Based on hypotheses

Table 6-18: Difference between Standard Analytic Approach *versus* Red Team as Envisioned in DIOCC/JIOC Red-Team Construct[184]

Despite this greater visibility, funding, and new found relevance, the term *red team* is suffering from what Cordray (2007) calls 'definition creep.' Potential customers of analytic red-team products are unsure of red-team purposes and processes and therefore question their value and credibility.[185] There are numerous definitions of the term and one of the key problems this study seeks to address is the development of descriptive taxonomy that can benefit the red-teaming community at DIA and other practitioners.

Other COCOM JIOCs have sought to address these issues and others with their red teams. Kibiloski (2009) and others have been conducting road shows and outreach activities to COCOMs and others within the community. Sometimes a definition of what the construct isn't is as helpful as what it is—In Cordray's *Collaborative Analytic Red Team Processes* (2007), he defines what the DIOCC/JIOC red-team construct does not do to assist with an understanding of what it *is* designed to do:

What the Red Team Doesn't Do --[186]
Act as Operational Forces (OPFOR)
Not driving *Red* moves or countering *Blue* ones (We are "Blue's Red")
Conjure up unorthodox (i.e., crazy) ideas
Will explore low probability/high risk ideas, not off-the wall ones
Assess *Blue* Measures of Effectiveness (this is a *Blue* construct – and a big job)
Duplicate or frustrate JIOC work
Mission is to add value, not criticize analysts or planners
Identify/exploit *Blue* technical vulnerabilities
No phone-tapping, hacking

The DIOCC/JIOC red-team construct promotes those trained at UFMCS to facilitate, clarify assumptions, provide focus, promote creative idea generation and courteous discussion and argumentation. Unlike the NWC ONI DET red teams, the DIOCC/JIOC red-team model seeks to actually be "*Red" Centric*–to focus on perceptions and perspectives of the modeled entity, to mitigate analyst bias and mirror imaging, and to readily provide the adversary perspective.[187] Not just for *a* Command adversary but for *the* adversaries. The DIOCC/JIOC red-team model is seeking to address the problem of COCOM and war fighter organizational bias--to mitigate it and produce creative ideas through fresh perspectives, and to apply innovative analysis. As stated earlier, funding limitations have minimized the standup of JIOCs in COCOMs and the collection of metrics.

In engaging in COCOM analytical requests and planning support, Table (6-19) below depicts the three key DIOCC/JIOC red-team mantras and the RTL duties to maintain momentum both within the command and with external partners, intelligence and defense community members, and international or coalition entities.

IN CONDUCTING EXERCISES	RTL DUTIES
FACILITATE Clarify assumptions, provide focus, promote creative idea generation and courteous discussion and argumentation	The RTL is responsible for championing red team capabilities within operational elements, DOD, and Intelligence Community
THINK DIFFERENTLY As a devil's advocate, challenge assumptions, consider overlooked possibilities and emerging issues	The RTL, in consultation with DIOCC senior staff, is responsible for defining operational constraints for red team involvement including desired classification levels of findings, collaboration with partner nations, and intended product uses.
Think "RED" by: Analyzing and predicting adversary (Red) and other (Green) perspectives, perceptions Identify secondary, tertiary and unintended effects of Blue actions in a cultural context Contribute Red and Green perceptions of Blue to COCOM strategic communications	The RTL will schedule and facilitate collaborative Red team efforts as required to meet the needs of the JIOC Enterprise.
Reach out by--Leveraging analysts, scholars, think tanks and contractors to build issue-focused Red teams Interact often with non-Blue institutions, cultures, and countries in COCOM X AOR Understand COCOM X processes, personalities, priorities Network with other Red teams for lessons learned, best practices	The RTL will produce papers, briefing and other products as required documenting Red team findings.

Table 6-19: Key DIOCC/JIOC Red-Team Approaches while Conducting Exercises & RTL Duties[188]

The DIOCC/JIOC red-team construct also appears to be playing a valuable role throughout the planning, execution and review of war games and exercises. In a pre-exercise environment, the DIOCC red team often participates in the planning process and challenge concepts and assumptions used in building scenarios, especially as they portray an adversary and other actors. During COCOM exercises, JIOC red teams have provided inputs on adversaries and other perceptions and likely reactions to friendly communications and actions. Post-war game/exercise, the red teams critically review exercises, which includes the exercise processes, assumptions and chosen courses of action to explore alternative processes or outcomes and refine future planning.[189]

Table (6-20) shows some of the tools, techniques, and procedures (TTPs) that the DIOCC/JIOC red-team construct applies and the disciplines that contribute to the TTP based on discussions with red-team SMEs from DIA and the COCOM *X*.

DISCIPLINES INVOLVED	TOOLS, TECHNIQUES, AND PROCEDURES (TTPs)
Military History, Economics, Mathematics,	Structured Brainstorming –A facilitated, focused approach that adheres to ground rules and often employs visual aids or other idea stimulating material
History, Economics, Natural Sciences	"What If" Analysis –Takes as a given that an event has occurred, then 'think backwards to how it could have come about
Engineering, Economics, Mathematics	Structured Analogies –Systematically identifies and rates analogous situations to forecast future problems and discover the most possible outcomes of a given situation
Mathematics, Philosophy, Religious Studies, History, Law	Extreme Users –A method by which a variety of participants are selected based on their expertise, or lack thereof, on the subject being discussed –"inside the box", "outside the box", and "unaware of out of the box thinkers"
Engineering, Military History, Social Sciences	Human Factors–A method by which psychological, ethnographic, or cultural profiles are used
Cultural Studies, History, International Relations, Social Sciences, Political Science	Entity Mirroring –A method by which the analytic team is selected by their similarity of the modeled entity; such as hiring members of the adversary team or individuals with adversary skills or insider, first-hand knowledge
Cultural Studies, Military History, International Affairs	Cultural Immersion –A method by which participants experience stimulus material designed to produce a degree of paradigm shift and inculcate a greater understanding of the adversary's perspective.

Table 6-20: Key JIOC Red-Team Disciplines matched to TTPs[190]

UFMCS and DIA briefings have stated red-team participation is ideal for the development of a comprehensive COCOM strategy and more thorough concept development. The DIOCC/JIOC red-team construct is designed to provide the historical, ideological, political, and cultural context in which to investigate the complex dynamics of cause-and-effect, including second and third order effects, in response to blue strategic actions. Respondents stated this insight enables the J-2 Commander to understand the broad long term impact of alternative courses of action relative to achieving the desired strategic intent and influence the COCOM.[191]

The DIOCC/JIOC construct is intended to contribute to policy development by identifying cascading effects of actions resulting from proposed policy and/or identifying missing elements of policy that needs to be addressed. For new policy development, COCOM *X* red teams are engaged in the review of publications to ensure proposed positions are founded on assumptions and facts that are free from biases, mirror imaging, and insensitivity to historical, political, and/or cultural perceptions of adversaries, friendly forces, or non-combatants. For existing policy, a DIOCC/JIOC red team may be called upon to review current positions with respect to new world event, trends, and threats in collaboration with policy organizations to assure that policy remains consistent with the operational environment and coordinated among joint publications and other joint documents.[192] In all cases, the COCOM policy organization

will adjudicate red-team comments and incorporate into the larger organizational response, or dismiss with commentary.

6.5.7 DIOCC/JIOC Construct Measurement/Metrics

Strategic and operational-level assessment efforts concentrate on broad tasks, effects, objectives, and progress toward the military end state. Continuous assessment helps the COCOM and U.S. military Service joint force component commanders determine if the joint force is "doing the right things" to achieve objectives, not just "doing things right." The JFC also can use red team-developed methods of effectiveness (MOEs) to determine progress toward success in those operations for which tactical-level combat assessment ways, means, and measures do not apply. Intelligence analysts use the JIPOE process to assist in the identification of desired and undesired effects and the development of related MOEs by analyzing adversary COAs as advanced by the red team, as they relate to the friendly mission, end state and objectives.

Table (6-21) below lists some of the key tenets taken from both Cordray (2007) and Kibilowski (2007) to define the philosophical underpinnings of the DIOCC/JIOC approach to red-teaming.

DISTILL OUTPUTS/RESULTS	SUCCESSFUL DIOCC/JIOC RED TEAMS
Series of findings based on formulas, quantitative and qualitative analytical components assess approaches to problems before a decision is made	Not driven by daily events or production requirements; Maintains strategic, long-term outlook; self-initiates much of work; Small, dynamic team with diverse expertise and experience; Robust interaction with Blue – while maintaining autonomy; Not vested in particular methods, processes, organizations, outcomes or what is being evaluated; Direct leadership access, top cover and buy-in; Limited bureaucratic vetting allows for timely products; Communicates effectively and early; Confrontational with ideas, not people Intended audience understands Red team's mission, purview; Provides ideas early enough to be incorporated, not after-the-fact criticism; Operates within its organizational culture, which needs to be open to new ideas, criticism; No standardized Tactics, Techniques, Procedures (TTP); doctrine; Clearly defined CONOP avoids mission creep, sets expectations; Education in anthropology, critical thinking, theory helpful but not required

Table 6-21: Key DIOCC/JIOC Philosophical Tenets[193]

According to Cordray (2007) red teams are particularly valuable in identifying and developing indicators (which may be used as the basis for MOEs) to monitor changes in

adversary system behavior, capabilities, or the operational environment. Red-team support to assessment encompasses all aspects (political, military, economic, social, informational, and infrastructural) of the operational environment.[194]

Table (6-22) shows the outputs or performance indicators the DIOCC/JIOC red-team construct is capable of providing on a measurable basis.

OUTPUTS/RESULTS TYPE	MANIFESTATION
POLICY DEVELOPMENT ASSESSMENTS	Contributing to military operations "Red View" on *COUNTRY A* senior leadership thinking after cyclone hit cited by AmEmbassy *COUNRTY A* capital, resulted in validated red team assessment
PLANNING, ASSESSMENTS	HA/DR Joint Task Force in *COUNTRY B* as valuable contribution to their efforts to gain access, provide aid to Delta region of country which prompts re-validation of assessments
POLICY DEVELOPMENT ASSESSMENTS	Alternative assessment on the terrorist threat to the Olympics elicited interest at the Deputy Assistant SecDef level, prompted primary reporting organizations to re-examine credibility of their sources Providing relevant non-military, non-Intelligence Community perspectives
POLICY DEVELOPMENT	Partnered with literary critic and professor from *COUNTRY C* in writing alternative analysis on *COUNTRY D*; unique, thought-provoking perspective elicited Intelligence Community discussion
WARGAMING/EXERCISE SUPPORT STRATEGY AND CONCEPT DEVELOPMENT PLANNING	Support Command exercises; Provided "Red/Green View" to COCOM Commander during annual staff exercise, thus building a reputation
WARGAMING/EXERCISE SUPPORT STRATEGY AND CONCEPT DEVELOPMENT PLANNING	DIOCC/JIOC red team visibility in the Command is rising, there is greater understanding of what RT does, products are widely read, analysts now come to us with ideas Positive feedback from senior COCOM leadership and beyond - Director of Naval Intelligence, Strategic Command (USSTRATCOM) J-2, Office of the SecDef for Policy (ASP[P])
STRATEGY AND CONCEPT DEVELOPMENT PLANNING, POLICY DEVELOPMENT	RT products finding their way into a Combatant Command commanders or Joint Chiefs read-ahead package (called a readbook by the Assistant Secretary of Defense [ASD])
STRATEGY AND CONCEPT DEVELOPMENT PLANNING, POLICY DEVELOPMENT	Providing updates to joint pubs, Rewriting 33-14 Intelligence Planning docs
STRATEGY AND CONCEPT DEVELOPMENT PLANNING, POLICY DEVELOPMENT	Rewriting JCS memo, JCS takes RT recommendations, JCS changes behavior
STRATEGY AND CONCEPT DEVELOPMENT PLANNING, POLICY DEVELOPMENT	07 strategy change in OIF based on assessment done by DIOCC/JIOC RT
STRATEGY AND CONCEPT DEVELOPMENT PLANNING, POLICY DEVELOPMENT	Successful execution of Operational Plans
WARGAMING/EXERCISE SUPPORT STRATEGY AND CONCEPT DEVELOPMENT PLANNING	DIOCC enterprise red team Concepts of Operations (CONOPs) documentation
STRATEGY AND CONCEPT DEVELOPMENT PLANNING, POLICY DEVELOPMENT	J-2 (Intelligence) feedback via formal accommodations or informal emails, informal "attaboys"
STRATEGY AND CONCEPT DEVELOPMENT PLANNING, POLICY DEVELOPMENT	Joints Chief Of Staff incorporates recommendation into policy, speeches, direction, COCOM Standard Operating Procedures, etc.
ASSESSMENTS	Red Team products find their way into other Intelligence Community documents or Intelink

Table 6-22: Key JIOC Red-Team Performance Indicators[195]

The DIOCC/JIOC red-team process had very explicit metrics thought out that either validated red-team contributions to the command or focused on lessons learned to

make them better contributors. This fact could have been because of respondents' expertise or its emphasis in the COCOM *X*. As one peruses the manifestation of red-team success definitions, the reader can see that red-team products can have an effect on diplomacy, economics, politics, and a number of secondary red team and intelligence analyses efforts. That may be why DIOCC respondents spoke of the criticality in creating a red-team "community" to pull in other DoD agencies, coalition partners, other foreign elements, and members of the diplomatic and intelligence communities.

Kibilowski (2009), Cordray (2007), and DIOCC/JIOC red-team member survey respondents discuss the need for increasing full access to people and information. Staff actions and planning activities must ideally be transparent to red-team members, and data necessary to accomplish red-team tasks must be available if the team is to provide viable and timely value added.[196] This is not always the case due to geographically dispersed COCOMs, funding limitations, and some COCOMs that do not understand or believe in value of an embedded cadre of red-teamers. Additionally, to engage in a project and allocate necessary resources, authority must be decentralized to the lowest appropriate level (e.g., the RTL). This decentralization philosophy demands highly competent red-team members that can seize opportunities to make important contributions.

6.5.8 DIOCC/JIOC Comparisons to the DoD/Military Model

For the DIOCC/JIOC red-team construct to be effective, it must be flexible, autonomous and, simultaneously, closely imbedded within DIOCC and for the JIOC, COCOM operations. It requires a broad CONOPs and a defined set of TTPs and Standard Operating Procedures (SOPs), which is contrary to U.S. military and organizational culture.[197] Further, the wide array of definitions and roles for red teams/red cells can complicate the team's effectiveness. For example, some outsiders assume a red team is acting to penetrate systems or technologies (a Sandia National Laboratories red-team function)– which is *not* a DIOCC/JIOC red-team function. Others assume the red team

is OPFOR – which can be the case (it is in the NWC ONI DET red team for example), but is often NOT the role the DIOCC/JIOC red-team construct is fulfilling.

Given the red-team's mission of questioning assumptions, providing alternatives and conducting critical review, the team could be viewed as a hindrance (rather than a help) to staff processes and progress. It is only with the trust and confidence of the DIOCC leadership that the red team is given top cover, access to the people and information that it needs, and the autonomy required to maintain its impartial perspective.[198]

The DIOCC/JIOC red-team construct must be sufficiently connected to DIOCC and COCOM leadership in order to identify critical relevant issues, such as key decision points, analytical perspectives, operational implications, planning concerns, command priorities and organizational tempo.[199] Simultaneously, the DIOCC red team must sufficiently be separate from the DIOCC staff processes to escape bureaucratic hindrances and the gravitational pull of organizational groupthink to provide alternative and longer-term strategic perspectives.[200]

DIOCC/JIOC red teams are a critical tool in allowing a Combatant Commander's (or RTL's for that matter) ability to understand the adversary and visualize, anticipate, and plan for relevant aspects of the operational environment. The construct is dependent on UFMCS training its red-team members and as stated earlier, and the receptiveness of the individual COCOM leadership including the J-2 (intelligence) two star admiral or general; and is an embedded decision support and planning tool not an opposing force (OPFOR) as the ONI DET red-team model. The DIOCC/JIOC red-team model is an operational demonstration of the UFMCS graduates in action. The model provides Combatant Command staff and especially the J-2 with additional adversary information that he/she might not have had to make a better informed rational decision. This model follows in the DoD/Military red-team decisionmaking model which may not account for non-linearity or non-traditional adversaries who employ civilian or irregular warfare operations.

6.6 Sandia National Laboratories (SNL)

As one of the premier Federally Funded Research and Development Centers (FFRDC) in the United States, U.S. government program offices such as the Departments of Energy, Defense, and Homeland Security, request Sandia's support in developing advanced technologies and systems that transform some agency functions, operations, or activities into more effective, efficient systems while enhancing survivability. SNL is involved in a number of joint red-teaming and vulnerability assessment efforts with government agencies. As the prime contractor for the federally funded National Infrastructure Simulation and Analysis Center (NISAC), SNL has jointly developed the NISAC as a modeling, simulation, and analysis program that prepares and shares analyses of critical infrastructure and key resources including their interdependencies, vulnerabilities, consequences of disruption, and other complexities to sponsoring agencies. NISAC is classified as an FFRDC under the direction of the Department of Homeland Security's (DHS) Office of Infrastructure Protection (OIP).

6.6.1 Sandia National Laboratories National Infrastructure Simulation and Analysis Center (NISAC)

NISAC's goal is to strengthen customer national security goals by anticipating and delivering high-impact solutions to challenging problems facing the Departments of Defense, Homeland Security, and other federal agencies. NISAC is attempting to accomplish this role through the application of various modeling and simulation frameworks and methodologies to conduct wide ranging tasks such as helping maintain weapon systems superiority, developing complex adaptive systems (e.g. robotics), system-level modeling and simulation, assessment of technical, economic, and national-security implications of infrastructure protection, mitigation, response, and recovery options, critical infrastructure modeling, information-technology security, and homeland defense & force protection.

NISAC-Sandia also engages subject matter experts from related groups mentioned above with other experts such as physical security, special forces, law enforcement and other domains to bring together different technical areas from to ensure analytical rigor in NISAC recommendations or what the NISAC calls Physical Protection Systems (PPS).

6.6.2 Red-Teaming within NISAC's PPS Risk Management Paradigm

The term "red team" is more of a military term that is not regularly part of NISAC's lexicon. Other Sandia labs use the term *red team* including the *Information Operations Red Team and Assessments*™ (IORTA™) and the Information Design Assurance Red Team (IDART™) model (see Section 2) has been performing assessments for a variety of customers including government, military, and commercial industry. Through its participation in a variety of government programs and leadership of industry conferences, the IDART team has assembled a standardized theory and practice of red-teaming. IDART, part of the Information Systems Analysis Center at Sandia National Laboratories, continues to perform assessments to acquire an independent, objective view of customer weaknesses from a range of adversaries' perspectives. At the same time, the Center applies the IDART methodology principally to cyber systems which is not the focus of this study.

NISAC is the Sandia component, for the subject of this study, that utilizes red teams, or more accurately in SNL grammar; *threat (an undefined negative resource); adversary (defined threat who wishes harm to a system)*, or *attacker (group of adversaries with goal to disrupt a system)* teams that are used to flesh out and define a threat as it relates to each subsystem of the (macro) system assessed to rank overall targeted system risk.

NISAC has substantial adversary threat experts in house (see Garcia, 2007) but also subcontracts subject matter experts for its Vulnerability Assessment (VA) evaluations to augment its VA Teams when subject expertise is required based on the systematic

evaluation objectives and requirements of a particular study. Given the fact that the methodologies used by NISAC are generally systems centric (PPS) risk-based, and algorithmic in nature—e.g., based on a series of standardized calculations for such items as security systems, sensors, alarms, alarm communications and displays, entry control, delay, response, communications system, on-site personnel; *red-teaming* is not a phrase used regularly by the NISAC. However, experts in the previously mentioned subjects may be brought into a study and expected to contribute to qualitative and quantitative calculations such as whether the threat definition models are planted in the workforce, native elements (if the facility is in a host country), sleeper cells, special forces or foreign military. See Table (6-23) for additional information on NISAC's Key Risk Management Paradigm and where the vulnerability assessment fits in that particular vulnerability framework.

METHODOLOGY COMPONENTS	FUNDAMENTAL DEFINITIONS	MENTIONED BY RESPONDENT
Risk Management	Set of actions an enterprise takes to address identified risks and includes avoidance, reduction, spreading, transfer, elimination, and acceptance options	Referenced in Garcia text
Categories of Risk (Assessment)	Market, Credit, Strategic, Operational, Liquidity, Hazard; Analyst must answer three questions: (1) what can go wrong?; (2) What is likelihood that it would go wrong?; (3) What are the consequences?	No
Hazard Risk	Specific category of risk related to security and assumes knowingly Determining existence of hazard rather than unwitting acceptance—Answers second set of questions: (4) What can be done?; (5) What options are available?; (6) What are their associated trade-offs in terms of costs, benefits, and risks?; (7) What are impacts of current management decisions on future options?	Referenced in Garcia text
Safety and Security	Two types of Hazard Risk Sub-categories--	No
Define Threats & Assets, (Risk Assessment)	Security Sub-category process of answering questions 1-3 above using *threat*, *likelihood of attack*, and *consequences of loss* as benchmarks	Yes
Vulnerability Assessment	Systematic evaluation in which quantitative or qualitative techniques are applied to predict physical protection system (PPS) component performance and overall system effectiveness by identifying exploitable weaknesses in asset protection for a defined threat	Yes
Products that are created by conducting the VA	Identified weaknesses that are used to establish the requirements for an upgraded PPS design; and can be used to support management decisions regarding protection system upgrades	No, but referenced in Garcia text
Either VA Process	Three distinct phases—*Planning; Conducting the VA; Reporting and Using the Results*	No, but referenced in Garcia text No
Physical Protection System	System that protects an asset or facility by *Detecting, delaying*, and *responding* to an adversary action against that asset	No, but referenced in Garcia text No
Threat Definition (In context of NISAC Paradigm)	Adversary class (insider, outsider, collusion between insiders and outsiders) Adversary goals (theft, sabotage, other goals such as workplace violence, sale of illegal drugs on site, creating negative publicity) List, collect, and organize adversary information	Yes and referenced in Garcia text

Table 6-23: Key NISAC Risk Management Paradigm

NISAC's vulnerability assessments process is the mechanism in which threats are applied to a system to calculate systemic risk. The evaluation techniques presented in the following section use a system performance-based approach to meeting the PPS objectives. The primary functions of a PPS are to create a cost-effective and efficient framework that can detect, delay, and respond to a threat that becomes an adversary by acting against the targeted facility. There are quantitative and qualitative methods of evaluating PPS components at a facility based on the VA.[201] The VA threat *team* is basically a red team charged with determining the best methods to attack a facility given a defined group of constraints, assumptions, and objectives and reports their results. The PPS combines these results data with quantitative methods (qualitative when not enough quantitative data is available) and against facility characteristics, (such as walls and remote location), physical protection systems, (such as alarms, guard towers, and sensors), and analyzes, assesses, and evaluates the PPS risks, design, and consequences of loss.[202]

Garcia (2006) states that most facilities or enterprises routinely conduct risk assessments of their security systems to verify that they are protecting corporate assets and to identify areas that may need additional attention.[203] Such assessments are defined differently by differing enterprises, but in general they include consideration of the likelihood of a negative event, in this case a security incident and the consequence of that event. Garcia has outlined previously (2001)[204] a description of (security) risk assessment and provided a formula that can be used to calculate risk, using quantitative or qualitative measures. Security risk can be measured through the use of the following equation:

$$\text{Risk} = \text{Probability}_A * (1 - P_E) * C$$

Where R equals risk to the facility (or stakeholders) of an adversary gaining access to, or stealing, critical assets. Range is 0 to 1.0, with 0 being no risk and 1.0 being maximum risk. Risk is calculated for a period of time, such as 1 year or 5 years. P sub A equals probability of an adversary attack during a period of time.[205]

$$P_E = P_I * P_N$$

Probability sub E equals probability of interruption by responders multiplied by the probability of neutralization by first responders. P sub N is the probability of neutralization of the adversary given the interruption.[206] P sub N can include a range of tactics from verbal commands up through deadly force. The appropriate response depends on the defined threat and consequence of loss of the asset.

C equals consequence value. A value from zero to one, that relates to the severity of the occurrence of the event. This is a normalizing factor, which allows the conditional risk value to be compared to other risks across the facility. A consequence table of all events can be created which covers the loss spectrum, from highest to lowest.[207] By using this consequence table, risk can be normalized over all possible events.

At the Department of Defense and SNL-sponsored Threat Metrics Workshop--*"What information helps you anticipate your adversary?"* the Red Team 2007, presenter Adventium (2007) posited that risk can be expressed as:

Risk = Consequence X Probability

However, an alternate formulation is widely offered for threat-based risks:

Risk = Consequence X Threat X Vulnerability[208]

So there is some common agreement that systems risk is a product of an equation of probability over time and severity of consequence in an equation. Additionally, probabilistic risk assessment focuses on the more formal, scientific, technical, quantitative, and objective when compared to risk management and red-team heuristics-- which is more subjective, qualitative, social, and political.

6.6.3 NISAC Threat/Adversary/Attacker As Defined within the VA Design Process

In a perfect risk model, the use of probabilities is based on objective likelihoods, but in the security domain, it is common to use more subjective likelihoods based on intuition, expertise, partial, defective, incomplete, or erroneous intelligence data.[209] This is critical because these data are major sources of uncertainty and uncertainty is a major element of risk. According to Garcia (2007), these measures can reduce credibility of the risk assessment and exacerbate the chronic lack of dependable (that is, quantifiable) data for adversary attacks.[210]

The risk equation in Section 6.6.2 can be used to determine the security risk life cycle in context. When considering security systems and the attack timeline, the attack can be broken down into three discrete phases: pre-attack, which is the time an adversary takes to plan the attack; the attack phase, when the adversary shows up to attack the facility; and post-attack, when the adversary has completed the attack and the consequences of a successful attack occur.[211]

However, before the attacker can be specifically defined, it must be quantitatively derived from a VA process. The VA process first requires a determination be made of PPS objectives. These can be enhanced facility characteristics; or defined defense against a spectrum of threats; or PPS targets or standards identified. Then a PPS is designed with a series of detection, delay, and response subsystems based on economic or budgetary constraints. After determination of PPS objectives and PPS characteristics, an analysis of the PPS design is conducted and from that analysis comes a series of final PPS design criteria or a redesign of an existing PPS. Table (6-24) shows the threat definition (red-team development) in context of a standard VA process.

VA DEVELOPMENT SUB PROCESSES (From NISAC Respondent and Garcia)	STEP IN OVERALL VA PROCESS
Phase 1: Plan project	Determine PPS Objectives
Initial customer contact	Determine PPS Objectives
Define project	Determine PPS Objectives
Particular vulnerability/issue/VA is selected by customer	Determine PPS Objectives
Phase 2: Manage project	Administration/Staff
Maintain project status and reporting mechanisms	Administration
Phase 3: Establish vulnerability assessment team	Determine PPS Objectives
Project leader	Administration/Staff
systems engineer	Administration/Staff
security systems engineer	Administration/Staff
SME-intrusion sensing subsystem	Administration/Staff
SME-alarm assessment subsystem	Administration/Staff
SME-alarm communications & display subsystem	Administration/Staff
SME-entry control system	Administration/Staff
SME-delay subsystem	Administration/Staff
SME-response subsystem	Administration/Staff
SME-communications subsystem	Administration/Staff
SME-analyst	Administration/Staff
Kick off mtgs	Administration/Staff
project team kick off mtgs	Administration/Staff
VA team guide	Administration/Staff
site info print out	Administration/Staff
customer kick off mtg	Administration/Staff
Phase 4: VA Process	**Design PPS**
List info needed to define threat	**Design PPS**
Collect info on potential threat	**Design PPS**
Organize info to make it useable in VA	**Design PPS**
Threat definition methods--	**Design PPS**
develop threat from historical or intelligence data	**Design PPS**
Use a policy-based threat issued by appropriate agency or organization	**Design PPS**
Create a range of potential threats (threat spectrum)	**Design PPS**
Insider threat (passive, active, irrational, rational, nonviolent, violent)	**Design PPS**
Other notes on threat definition	**Design PPS**
Estimating likelihood of attack	**Design PPS**
ID Assets	**Design PPS**
Perform facility characterization	Analyze PPS Design
4 Path Analysis	Analyze PPS Design
4a Build particular set of modeling tools for a facility --for example	Analyze PPS Design
4b Factor in and set algorithms for layers of security (i.e., fence, wall, building structure itself)	Analyze PPS Design
5 Vulnerability assessment analysis	Analyze PPS Design
5a examine physical structure	Apply Red Team
5b ID weaknesses	Apply Red Team
5c hardened structures/delayed response	Apply Red Team
5d frontal attack algorithms	Apply Red Team
5e sneak attack algorithms	Apply Red Team
6 Red team approach	Apply Red Team
6a Assemble two teams	Apply Red Team
6b non permissive team environment (covert operations)	Apply Red Team
6c Permissive team environment	Apply Red Team
6d Team one (SOF) Determine requirements for breaching	Apply Red Team
6e team One; Determine data needed	Apply Red Team
6f Collect data on team one	Apply Red Team
6g Second team (natives) Determine rqmts for overt breaching	Apply Red Team
6h Team Two: Determine data needed	Apply Red Team
6i Collect data on team two	Apply Red Team
7 Look at what team one would have to do with step 4 Path Analysis	Apply Red Team
8 Look at what Team two would have to do with Path Analysis	Apply Red Team
9 Look at what team one would have to do for frontal attack (VAssmnt)	Apply Red Team

10 look at what team two would do in frontal attack	Apply Red Team
11 Review actions of Team one in covert ops attack	Apply Red Team
12 Review actions associated with team two in covert ops attack	Apply Red Team
13 Develop set of scenarios	Develop Possible Scenarios
13a combat simulation hot wash	Identify Take-aways
13b force on force hot wash	Conduct Interactive Engagement Simulation
13c tabletop hot wash	Evaluate Take-aways
14 Provide different levels of granularity depending on view but have far more Detail than necessary to have available	Collect Lessons Learned
15 Report	Report out

Table 6-24: Key NISAC Vulnerability Assessment Process Steps
(With Threat Definition and Adversary Action Processes in Red and Administration/Staff activities conducted by SNL Program Management prior to engagement of red team)

6.6.4. Phase Four of the VA: Define Overall PPS Objectives

Phase four of the VA process involves three key sub-processes or methods that need to be further defined to understand the NISAC *red team* or *threat analysis* approach. These are *threat definition*, *estimating probability of attack*, and *asset identification and loss criteria*, and after potential threat information has been initially gathered, it should be organized to make it useable and to facilitate decisions concerning which threats will be included in the threat spectrum used to assess the effectiveness of the existing PPS. The threat definition may consider insiders, outsiders, and both in defining characteristics of types of adversaries needed to be part of a comprehensive threat definition.[212] Table (6-25) identifies how the establishment of overall protection objectives will bound the threat definitions in the NISAC VA process model below.

OVERALL PPS OBJECTIVE	RATIONALE
Defining the threat	Establishes the performance required from the PPS; by describing the threat, the assumptions that were made to perform the assessment are documented are used to show how they influence required upgrades.
Identifying assets and prioritizing them by consequence of loss	Asset identification is evaluation of what to protect by considering the value of the asset to the facility or enterprise. Three step process: 1-specify undesirable consequence; 2-select asset identification technique; 3-identify areas/components/material to be protected
Creating a matrix relating threats and assets	After threats are defined and assets have been prioritized, a considerable amount of information is generated that is used to establish protection system objectives
Characterizing a facility to perform a VA	The major part of the VA is the facility characterization—this consists of evaluating the PPS at the site. The goal of the VA is to identify PPS components in the functional areas of **Detection, delay,** and **response** and gather sufficient data to estimate their performance against specific threats

Table 6-25: NISAC Protection Objectives and Rationales

6.6.5 NISAC Threat Definition Methods (Design Basis Threat-DBT)

Threat definition (*possible red threat definition teams*) establishes the performance that is required from the PPS (or *blue team*). By describing the threat in detail, the assumptions that were made to perform the VA are documented and are used to show how they influenced required upgrades.[213]

Before the threat can be defined, information that would be most useful to know about the adversary must be understood. Typically, this information includes the adversary class (insider, outsider, collusion between insiders and outsiders) and their goals, motivation, and capabilities. Adversary goals could include theft, sabotage, other goals such as workplace violence, illegal activities on site, creating negative publicity about activities or ownership of the facility. Theft can include removing physical items or information. Sabotage may involve damaging critical equipment, release of hazardous material, or modification of data or proprietary information.[214]

The collection of threat information is accomplished by reviewing available documentation and by contacting agencies that may have useful threat information. These organizations could include local, state, federal, or military law enforcement agencies and related intelligence agencies. The following types of information may be reviewed for their use in defining threats:[215]

- Incident reports at the site
- A list of contacts for law enforcement activities
- The number of personnel at the facility and types of positions
- Reports of criminal or terrorist activities in the area
- Review publicly available information from sources such as the Internet, local newspapers, or professional associations and government sources[216]

After potential threat information has been gathered, it should be organized to make it useable, and to facilitate decisions concerning which threats will be included in the threat spectrum used to assess the effectiveness of the existing PPS. A table to assist in the organizing of the data is often helpful according to Garcia (2007).[217] Because the

threat definition will likely consider a wide range of threats, characteristics of many types of adversaries often are listed as part of the threat definition process. Table (6-26) below shows four useful methods used by NISAC to develop DBTs (defined basis threats) (Garcia, 2007).

THREAT DEFINITION[218] METHODS	ADVANTAGES	USE WHEN…	DISADVANTAGES
Develop threat from historical or intelligence data	Most common and easiest to develop with rigorous quantitative measures	Available statistics, historical data, exist and are attainable	Little historical data exists about a threat—e.g., terrorist threat to critical facilities
Use a policy-based threat	A specific group within an organization or intelligence agency creates a threat definition to address a policy question without revealing intelligence sources and methods that a specific threat definition would	Statistics about a specific threat do not exist in sufficient numbers or are classified to make a specific threat assertion	Sweeping policy statements may not allow efficient employment of defensive measures; nor relevant to most sites and forces many sites to adhere to standards that might be relevant to few
Create a range of potential threats (threat spectrum)	Allows an organization to define a range of likely threat definitions that focus PPS on more realistic threats and away from non credible threats	Little historical data exists about a threat to assist an analyst so organization selects/defines a range of capabilities or threats	Threat statement may offer more specific information whereas threat spectrum bay be too broad to offer actionable definitions
Use defined scenarios of adversary attack	Can achieve same goal as threat spectrum method but provides greater specificity and fewer possibilities; greater detail allows more information about adversary tools, capabilities, tactics, and techniques	Little historical data exists about a threat to assist an analyst so organization selects/defines a range of capabilities or threats	If scenario has too little detail, it can be weaker than threat spectrum method

Table 6-26: NISAC DBT Threat Definition Methods

6.6.6 NISAC Method for Estimating Attack Probabilities

According to (Garcia 2007), another crucial aspect of threat definition is estimating the likelihood of attack. The probability of this component of the VA process is difficult to determine. Historical data can be used to define the adversary; it can also be used to predict the probability of attack.[219] Garcia states that the probability of attack is really part of the risk assessment but many organizations want to know this as part of the VA.[220] The probability of attack may also be expressed as a frequency or likelihood. Garcia states these terms are often used interchangeably although there are some differences. Probability is the likelihood that a specific attack will occur, expressed as the ratio of the number of actual occurrences to the number of possible occurrences. Figure (6-5) depicts a simple method to estimate attack probability below.[221]

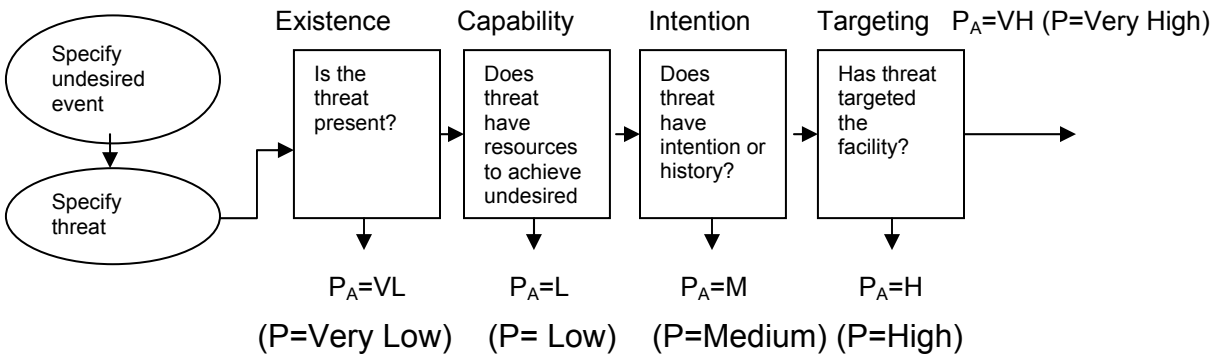


Figure 6-6: NISAC's Simple Method for Estimating Probability of Attack
(Based on Garcia's method)[222]

6.6.7 NISAC Asset Identification Methods & Loss Criteria

The final key sub-process in the NISAC threat analysis phase is the asset identification and consequence of loss criteria development. In addition to threat definition, the VA team must have an understanding of the assets to be protected. Asset identification is an evaluation of what to protect by considering the value of the asset to the facility, enterprise *or threat*. According to Garcia, there are three steps for identifying assets: (1) specify undesirable consequences; (2) select asset identification technique; and (3) identify areas, components, or material to be protected.[223] Table (6-27) shows the three key sub-processes.

THREAT DEFINITION	PROBABILITY OF ATTACK	ASSET IDENTIFICATION & LOSS CRITERIA
List information needed to define the threat	Specify event and threat	Specify undesirable consequences (damage to national security, terrorist attack, hazardous materials release)
Collect information on the potential threat	Determine threat existence, capability, intention, and targeting	Select asset identification technique (manual listing, logic diagrams, etc.)
Organize the information to make it useful	Develop probability product for each event	Identify areas/components/materials to be protected (consequence analysis/consequence of loss matrices)

Table 6-27: Three Key NISAC VA Sub-Process Inputs That Identify Threat as an Adversary

6.6.8 NISAC PPS Analysis Methodologies

Now that the threat has been identified as a series of adversary possibilities, the next step in the PPS that further requires red-team/adversary expertise is the analysis

phase. According to the NISAC VA of physical protection systems methodology, once VA data is collected, the analysis of the actual PPS can begin. There are two basic techniques for analysis—compliance based and performance based. Compliance-based approaches depend on conformance to specified policies or regulations; the metric for this analysis is the presence of specified equipment and procedures. Performance-based approaches evaluate how each element of the PPS operates and what it contributes to overall system effectiveness.[224]

The use of compliance systems is only effective against low threats, when assets have a low consequence of loss, or when cost-benefit analyses have been performed that show that physical protection measures are not the most cost-effective risk management alternative. A compliance-based analysis is easier to perform because the measure of system effectiveness is presence of prescribed PPS equipment, procedures, and people. The analysis consists of a review of facility conformance to the compliance requirements, the use of checklists to document presence or absence of components, and a deficiency report that notes where the facility is out of compliance.[225]

Garcia (2007) states that both qualitative and quantitative analysis techniques can be used in a performance-based analysis; the unique aspect to quantitative analysis is the use of numerical measures for PPS components.[226] The analysis process and techniques are summarized below in Table (6-28). There is always a recognized qualitative aspect to even a quantitative analysis but by using quantitative performance measures for PPS elements, much of the subjectivity of compliance-based and qualitative analysis approaches can be removed.[227]

When conducting either a qualitative or quantitative performance-based analysis, the six step process is used below:

ANALYSIS STEPS[228]	QUALITATIVE OR QUANTITATIVE?	RATIONALE
The Detection, delay, response instance outcome	n/a	PPS component performance
1. Create adversary sequence diagram (ASD) for all asset locations which estimates performance	Either	The ASD will show the steps the adversary takes to compromise asset
2. Conduct path analysis which results in values for P_I (probability of interruption)	Either	Software or storyboard documentation which results in defined probability of interruption includes review of defeat tactics
3. Perform scenario analysis which results in values for P_N	Qualitative	Analysis of scenario to review PPS versus adversary which will Determine values for neutralization
4. Complete neutralization analysis	Either	Analyzes values of neutralization includes add'l review of defeat tactics
5. Determine system effectiveness, P_E (probability of system effectiveness)	Qualitative	Derive effectiveness ratings
6. If system effectiveness, (or risk) is not acceptable, develop and analyze upgrades. $P_I * P_N$ equals P_E	--	P_E is output of the process

Table 6-28: NISAC Quantitative Analysis Approach Overview For Performance-based Analysis

The adversary sequence diagram (ASD) is a critical piece of the analysis process and represents what UFMCS, ONI Det, the DIOCC and JIOCs would consider the NISAC's *red-team* behaviors against the *blue team* or PPS. The ASD is a functional representation of the PPS at a facility that is used to describe the specific protection elements that are present. It illustrates the paths that adversaries can follow to accomplish sabotage or theft goals. Because a path analysis determines whether a system has sufficient detection and delay to result in interruption, it is conducted first. The path analysis uses estimated performance measures, based on the defined threat tools and tactics, to predict weaknesses in the PPS along all credible adversary paths into the facility. This step is facilitated through the use of an ASD of the facility to be analyzed.[229]

There are three basic steps in creating an ASD for a specific site:

1. Describing the facility by separating it into adjacent physical areas
2. Defining protection layers and path elements between the adjacent areas
3. Recording Detection and delay values for each path element

An example of these steps and the process of creating an ASD in illustrated below in Figures (6-7), (6-8), (6-9), and (6-10).

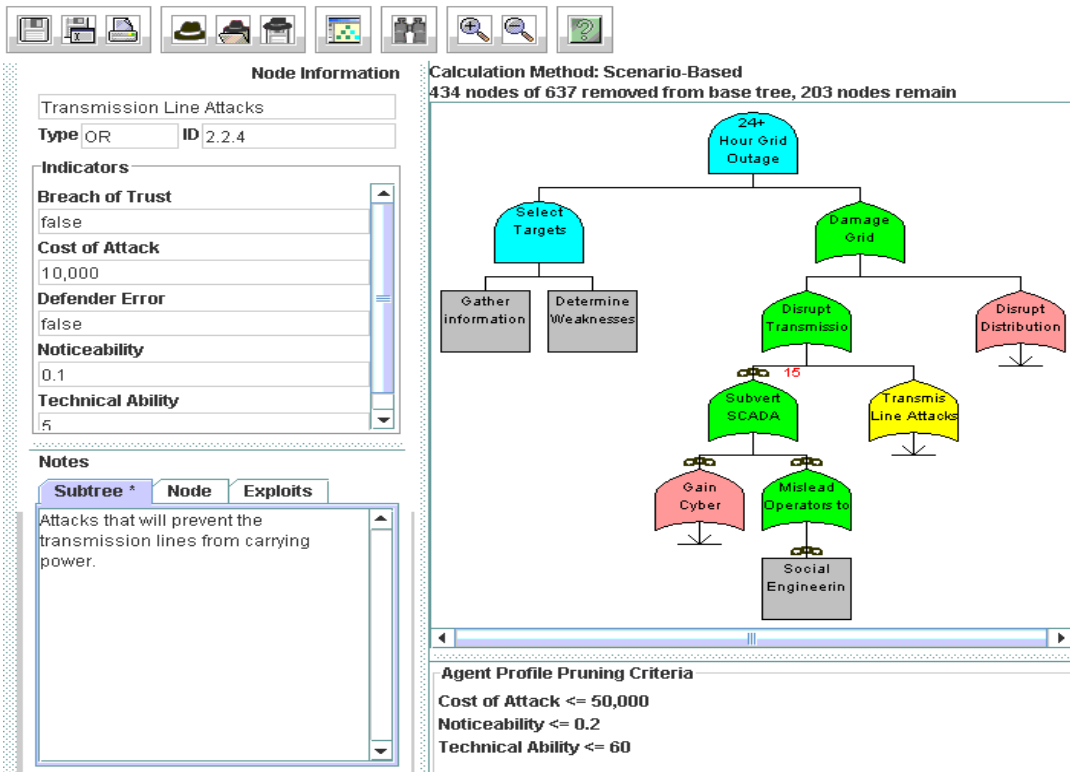


Figure 6-7: Transmission Line Attack Tree adopted from Threat Metrics Workshop: "What information helps you anticipate your adversary?"[230] Red Team 2007, 28-30 August 2007, Washington, DC

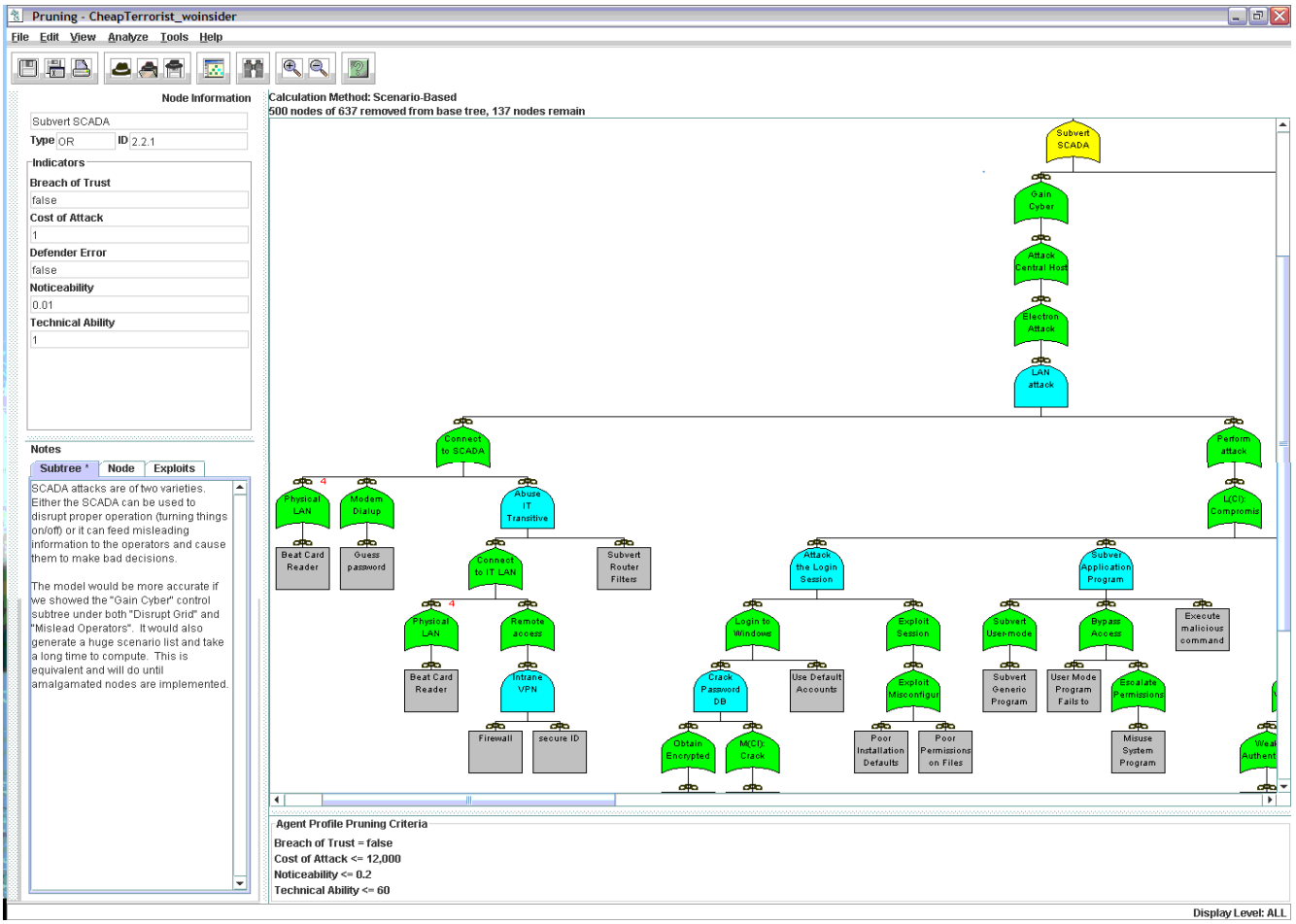


Figure 6-8: Supervisory control and data acquisition (SCADA)Tree adopted from Threat Metrics Workshop: "What information helps you anticipate your adversary?"[231]

As the reader can see from the ASD examples, the method basically depicts an attack in a format of an upside down tree. In fact the ASD is also called an "Attack Tree" which color codes the steps in the attack and the possible outcomes at each step. The text at the left of each illustration is a synopsis of the attack, its prospective cost, and other details and is not included in its entirety. Each figure is a different scenario displayed using software that highlights the whole sequence of events to sell the particular product. The reason for the inclusion in the study was to show the ability of software to capture the NISAC process of ASD development.

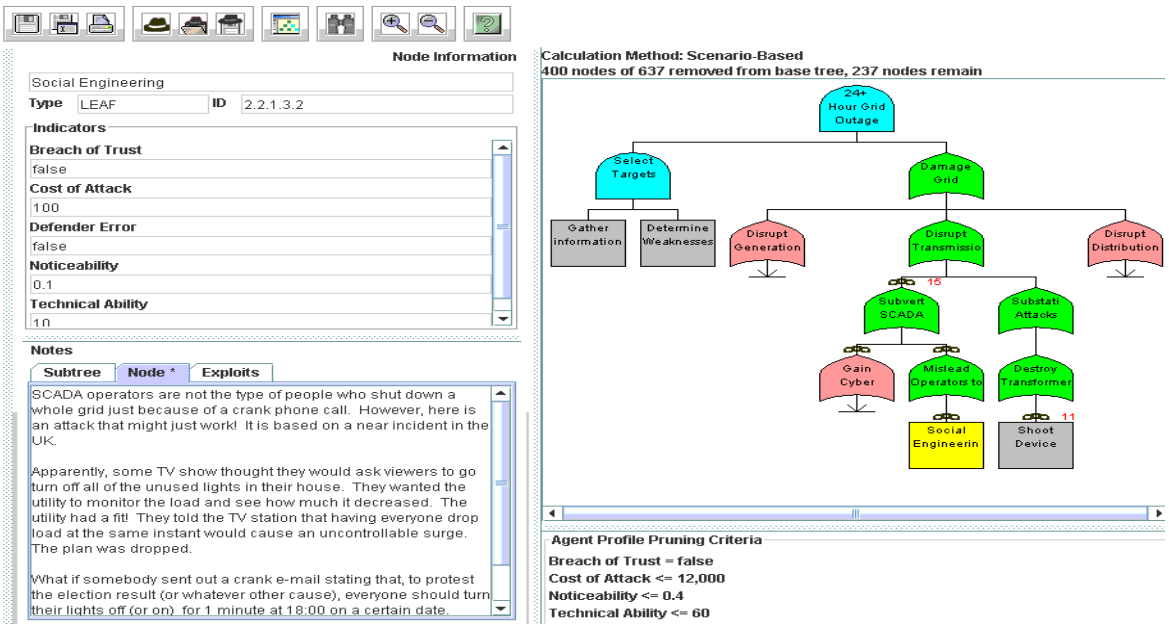


Figure 6-9: 24 Hour Grid Outage Based on Accidental Power Surge Attack Tree adopted from Threat Metrics Workshop[232]

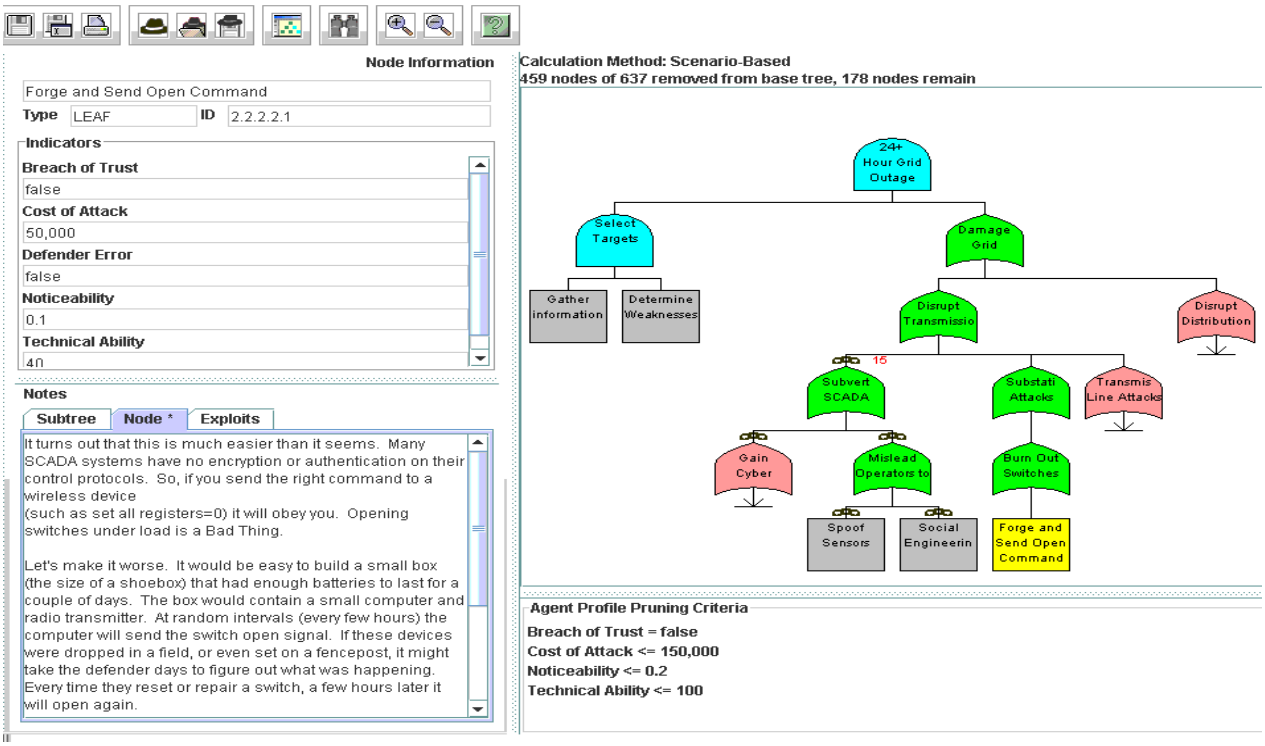


Figure 6-10: 24 Hour Grid Outage Based on Malicious Adversary Attack Tree adopted from Threat Metrics Workshop[233]

The ASD represents adjacent areas of a facility using concentric rectangles and area names that correspond to the site. It models a PPS by identifying protection layers between adjacent areas. Each protection layer consists of a number of path elements (PEs), which are the basic building blocks of the PPS. A key point for developing ASDs, is that one ASD must be created for each asset (target location), unless the assets are co-located. At complex facilities, several critical assets may need protection, and ASDs should be developed for each unique location.[234]

Once the ASD is created, the analyst assigns detection and assessment probabilities, delay times for PPS elements under different facility states, and any additional notes for each path element. The values recorded are the estimates provided to by the VA team SMEs as a result of their evaluation. These estimates include P_C (probability of communication) and the response force time, when there is an immediate response. This is the initial step in the path analysis. Both entry and exit path segments can be modeled. The entry path segment is from off-site to the asset, and the exit path segment is from the asset back off-site.

The ASD represents all adversary paths to an asset; paths that are not credible are identified in scenario analysis. Although only some paths are credible for specific threats, representing the entire PPS on the ASD is recommended. This provides good system documentation, allows for faster replication of analysis in the event that threats increase, and facilitates sensitivity analysis (how well the system performs against high or lower threats). This simple functional view also provides additional insights about credible adversary paths, which could be missed if some path elements are omitted.[235]

The path analysis is used to provide an overall view of the robustness of the PPS. By studying the potential adversary paths and the estimates of path element performance, the analyst can quickly determine how effective the PPS is and where vulnerabilities exist. Path analysis also identifies the continuous data protection (CDP) capabilities for multiple adversary paths. During path analysis, the assumption is that interruption and

neutralization will occur at the CDP, although actual response strategy depends on the asset. The key objective of path analysis is to evaluate the PPS at a facility at a high level and Determine how well protected all assets are at all times.[236]

Analysis of the ASD will identify the paths with the lowest P_I (probability of interruption) which is the starting point for scenario development and analysis. A scenario analysis is conducted to determine whether the system has vulnerabilities that could be exploited by adversaries using varying tactics, resulting in lower effectiveness of the PPS. Some facilities use scenario analysis as a substitute for a defined threat, where they postulate attacks, then decide what equipment or capability is required to be successful. Analyzing the PPS using defined threats and then generating scenarios by looking at weak paths is the preferred approach to ensure that credible paths are not missed.[237]

Using the scenario, a task-by-task or layer-by-layer description is developed. This description should be detailed enough to provide a scenario timeline and enough information that performance estimates for sensing, assessment, communication, delays, and response can be made.[238]

At this point the analyst reduces all the possible paths to those that are most credible. Paths can be removed from the final mix as a result of a number of tactical issues. For example, a path that appears very weak (low P_I - probability of interruption), using element performance measures may not really be credible because there are a large number of responders on the other side of the door with the shortest delay. Of course some paths will be eliminated because the adversary does not have the equipment or other capability to attack some protection elements (i.e., thick walls and only hand tools) and this is another source of path removal.[239]

Once the path analysis is complete, scenario analysis begins. These steps should be followed to conduct the scenario analysis:[240]

1. Develop attacks and tactics designed to exploit weak paths. Consider attacks during different facility states using the defined threat and capability.

2. Modify performance estimates for path elements using these tactics or under these states.
3. Document the assumptions used and the results of the scenario analysis.

A scenario analysis is aided by the creation of adversary task timelines and the associated performance of any path elements along the path. Scenario analysis considers specific tactics along the path, as well as attacks on the PPS itself or on the response force. These tactics include stealth, force, and deceit, and they may be used individually or combined during a scenario.[241]

Other aspects of scenario analysis include consideration of what on-site tools or other equipment might be used by the adversary to aid in the attack. In addition to the adversary task times, immediate response times must also be determined. The response times depends on the specifics of attack timing and response procedures, but a general notion of how many responders will be responding to the area and at what intervals is an effective first step in response time estimates.[242]

After the scenario is defined, and the adversary task timelines are created, performance estimates of path elements are made for the path. Table (6-29) shows examples of an adversary task timeline and a performance estimate for an adversary scenario below.

EXAMPLE OF ADVERSARY TASK TIMELINE			**PERFORMANCE ESTIMATES FOR ADVERSARY SCENARIO**				
TASK:	TASK TIME (sec.) (cumulative)		Probability of : (interruption)	(Detection) X (attack success) =(attack Detection)			
Approach facility	n/a	0	TASK:	P_D	P_{A8}	P_{AD}*	P_I
Enter facility	80	80	Approach facility				
Traverse exterior area	10	90	Enter facility				
Breach building	120	210	Traverse exterior area				
Traverse interior (entry)	10	220	Breach building				
Acquire asset	60	280	Traverse interior (entry)				
Traverse interior (exit)	10	290	Acquire asset				
Exit building	10	300	Traverse interior (exit)				
Traverse exterior area	10	310	Exit building				
Exit facility	10	320	Traverse exterior area				
Leave vicinity	n/a	320	Exit facility				

Table 6-29: Examples of Adversary Task Timelines and Performance Estimates for Adversary Scenario[243]

After weak paths and suitable attack scenarios have been determined, a neutralization analysis can be performed. This part of the analysis is performed only at facilities

where there is an immediate response resulting in a face-to-face confrontation with adversaries. Neutralization analysis provides information about how effective the response will be under different attack scenarios and is a measure of response force capability, proficiency, training, and tactics. This analysis assumes that interruption has occurred. If the defined threat for an asset or facility includes adversaries who will use force to prevent the response force from interrupting or neutralizing, analysis should consider the likely outcome of that engagement. At high security facilities, computer simulations are used to quantitatively predict the probability of neutralizing violent adversaries after interrupting them. For other facilities, past records of successful responses to security incidents can be used to estimate P_N (probability of neutralization) or the results of tabletop exercises can also be used

6.6.9 NISAC Threat Definitions Metrics/Measurements

Once a VA is completed, there are a variety of responses that can take place according to Garcia (2007). The most common approach is for the facility to pursue improvement to the PPS and following the recommendations of the VA team. Upgrades to the PPS proposed during the VA are usually limited to functional improvements (i.e., performance upgrades that must be achieved to improve overall system effectiveness).[244] Some enterprises leave implementation of recommendations to the managers responsible for the facility while others implement incremental PPS improvements via policy changes or in a prioritized manner across their multiple sites.

In cases where the VA is the end of the project regardless of whether the recommendations will be implemented, there are certain activities that should be conducted to successfully close out the project. In addition to archiving and closing out all VA files, an internal team review of the project is conducted. Use of this technique according to Garcia (2007) is limited to large projects.[245] However this can be conducted quickly and consists of reviewing what went well, what could have been done better, what actions could have reduced project costs, and what additional support might have helped to do the project faster or more effectively.[246]

Other threat metrics workshops sponsored by NISAC and other private sector VA firms that have sprung up since 9/11 have listed example characteristics of good metrics. Some of these are listed below were discussed at a Red Team Threat Metrics Workshop--"What information helps you anticipate your adversary?" Red Team 2007 in Washington, DC: [247]

- Clear: Comprehendible, unambiguous, and distinct;
- Composable: Supports aggregation or decomposition;
- Immutable: Predictive even if the adversary knows the attribute and value is being observed;
- Measurable: Possible to measure and specify;
- Objective: Limited contention on results;
- Significant: Key drivers are usable, results support reasoning.

6.6.10 The NISAC Model Against Other Red-Team Models

Sandia's NISAC red-team approach is a contributing component in their vulnerability assessment methodology. Red-teaming or threat assessment at Sandia is just one factor and not necessarily a critical element (depending upon the study). Threat assessment at Sandia is part of a larger systematic evaluation that can include: both quantitative and qualitative techniques; predictors of physical security system component performance and overall system effectiveness; can identify exploitable weaknesses in asset protection for a defined threat; and is designed to support management decisions regarding physical security system upgrades.[248]

IORTA and IDART, however widespread, well-known, and in use, focus on cyber and information system security (see Section 2). The NISAC model is focused on vulnerability assessments of physical systems and therefore must take a more heterogeneous approach to threats and adversaries. In Information and IT security, the attacker may have many motives and even methods for hacking past the system protection firewalls, but once he is in, there are currently a finite number of responses to malicious viruses and codes, identity thefts, latent trojan botnets and spam, and other

destructive penetrating agents. The issue of cyber red-teaming is a fascinating one and should be the subject of follow-study. This dissertation focused on red teams involved in social studies related to human and national security dynamics and not necessarily the systems engineering IT domain. However the differences between the two are shrinking as humans devise more ways to defeat information systems.

The NISAC model is extremely quantitative and detailed in comparison to the previous three DoD/Military red-team case studies. It would be very interesting to apply some of the UFMCS or ONI/DET red team that involve force protection systems and threat assessment into the NISAC vulnerability assessment structure and see if similar results are derived. This is a promising topic for further red-team study.

Chapter 7. Conclusions

7.1 Study Summary

The study purpose was to identify and compare what four organizations who conduct red-teaming analysis actually did to design and develop; apply or conduct; and measure to improve their red teams. Upon further analysis of their red-team drivers, processes, and outputs, UFMCS and DIOCC/JIOC are very similar in that they part of the same process. Based on lessons learned from current overseas contingencies, UFMCS is developing red teams that support commander decisionmaking, these red-teamers apply their trade at the commands they are assigned in the DIOCC or at a COCOM JIOC. The ONI/DET model is more of the classic red team one thinks of when the term is understood i.e., the group of intelligence and military professionals who set up the adversary and then "play" him against the blue team. ONI/DET is the classic threat emulator red team. The Sandia NISAC approach applies a series of algorithms to various threat definition models within the specified scope of the vulnerability assessment based on the overall PPS objectives.

The UFMCS and DIOCC/JIOC processes are similar and based on the specific command situation or operational environment (OE). All steps are derived from this OE and application of the self contained red team is conducted from what the threats are in this OE. Performance measurements are relatively informal and are based on keeping the commander from making a *bad* decision. A bad decision is defined as one that costs the command men, material, or excess effort for minimal gain based on the OE. The eight primary steps of this red-team approach are shown below in column two and four in Table (7-1).

Based on the findings in Section 5 of the development steps, a survey of the applications of red teams, and a standardized set of key characteristics, or if possible, a framework that puts into some context, the different approaches to red-teaming and constitutes a *methodology* to develop a successful (i.e., one that captures and validates

adversary behaviors, thought processes, approach to problem solving) red team for use by military and intelligence professional red-teaming developers across domains. (Eight steps were used and developed from the findings in Section 5 to better compare the four case studies.)

The ONI/DET model is more formal and requires more preparation time because it is driven by a government (usually military) sponsor who wants to see what happens when a specific scenario involving a plan, strategy, weapons system, resource proximity, or other condition is applied to a blue-team problem. As shown below in Table (7-1), the eight primary steps the ONI/DET red-team process are compared to the other studies in column three. Much of the preparation work is focused on getting the red-team SMART book ready to ensure the red team knows what they are to do in the exercise. Unlike the UFMCS and the DIOCC/JIOC red team, the ONI/DET has a much larger scope in that the sponsor may want almost anything red-teamed. Stated earlier, the ONI/DET process cannot account for non state actors so there are some limitations, but the ONI/DET red team prides itself on being able to handle multiple futures analysis, complex multilevel team interaction with non combatants, allies and coalition partners, and even new threats not yet in existence. Outputs are not actually measured or compared across discreet deliverables due to lack of staff resources but ONI/DET is so busy planning the next war game, if waiting lists are any indication of success, the DET is very successful.

The Sandia/NISAC process is harder to compare to the previous three red teams because the focus is on threat modeling for a comprehensive strategic decision support and threat emulation red-team methodology--not specific operational command decision support or threat emulation as in the previous red-team models. Now, UFMCS and the DIOCC/JIOC red-teamers would say their models are robust enough for strategic decisionmaking, but the NISAC model looks ten or twenty years in the future. The DoD/Military perspective is next week to perhaps five years out. Anything more cannot kill you today. The Sandia/NISAC threat definition modeling looks at what a wide spectrum of adversaries *could* do to you and then advises the leader of the enterprise

rather than tells the force commander what will harm him or her (UFMCS and DIOCC/JIOC model); or virtually engages in battle (ONI/DET model). As shown below in Table (7-1), the NISAC eight step process is a larger effort that contains just two or three sub-processes that contain the actual threat definition "red team".

Step	UFMCS	ONI/DET	DIOCC/JIOC	SNL-NISAC
1	Attend mission brief/review mission guidance and order; Begin data collection Based on staff planning timeline, develop p Receive/ recommend preliminary RT initial guidance from org. commander; Determine extra-org. requirements—if any.	RT need identified/ Red team needed-- call WG dept. to build action plan	Situational Development such as crisis, issue, etc./ Set the Scope –Establish the time frame, area of interest, and other boundaries or limitations based on the overall purpose of the assessment	Plan project
2	Independently from the staff, identify alternative end-states for US, coalition, and the adversary - based on Operating Environment (OE) variables; Cultural analysis of Operational Requirements (OR); Participate in planning & receive/ recommend preliminary RT initial guidance from commander	War-gaming Conference to identify key membership, & *Head* red team leader	Crisis Assessment; Review key attributes and effects of the operational environment –Examine characteristics of terrain and weather; strengths and vulnerabilities of infrastructures; capabilities and posture of blue forces; and influences of other entities	Pre-establish vulnerability assessment team either virtually or my lose confederation or community
3	Monitor staff development of COA. Analyze OR Independently develop COA based on projected objective, doctrine, capabilities, geography, and culture. Identify potential 2nd and 3rd order effects of friendly COA and actions	Planning conference to work out Details including red team issues, challenges, problems with adequate realism as defined by game director and staff.	COA Development/ Review known threat factors–Brief major findings of relevant threat assessments –Brief relevant human factors, if known	List info needed to define threat Collect info on potential threat
4	Help staff to decide if adequate measure Monitor war game to help ensure accuracy – (i.e., Ensure realistic capabilities are maintained; Evaluate appropriate actions and results; Balance operational requirements with other elements; Assist staff by serving as war game "umpire.")	Depending on game and RT involved, steps must be taken to ensure adequate realism and rigor or explanation of game limitations.	Red Team analyses mission/ Use structured idea generation to postulate WHAT could take place. (i.e., How can the adversary capitalize on his capabilities to achieve success?; How can historical analogous scenarios aid the adversary or this red team analysis?; What current terrorism or crime trends illuminate new adversary techniques?; What simple, counter defensive techniques might be used to overcome friendly security measures?; How might other entities affect the scenarios?	The red team lead considers the customer's core business questions, the types of red teaming involved, and types of relevant metrics to identify the set of targeted metrics needed for the assessment.
5	Monitor to ensure RT COA accounts for each of the identified OE variables	NWC reaches back to obtain experts on complex and/or little understood topics, religious subject,	Red Team war games issues/Assess which scenarios are most likely. –What cultural, social, or ideological factors might	The red team applies the targeted metrics to their assessment process. The metrics inform the process by helping guide

		historical issues, culture, etc.	influence the adversary's preference of one scenario over another? –Discuss Operational Viability –How might the adversary's view of the operational environment influence their adoption of a particular scenario? –Narrow and rate top scenarios, guarding against "blue teaming" or mirror imaging	the assessment's data collection, characterization, and analysis phases.
6	Conduct crosswalk to identify gaps, discon Linkage of staff actions to the end state Ke The Red team's value added is measured by the staff producing a better staff product and identification of alternatives to the staff and Commander	Red team staff elements or SMEs derived to put together red team Rules of engagement (ROE)/ Red team rules of engagement, etc. are Determined to understand how red team will operate, plan, execute, collect intelligence/analyze	Execution Planning/ Determine how a scenario might occur. –What steps will the adversary take leading up to execution of an action? –How will the adversary overcome challenges in the operational environment to achieve successful execution of the COA? –What is a viable tactical plan for the scenario including number of operatives, roles, tactics, weapons, plan synchronization/timing, and contingencies? –What elements of the adversary plan might be observable and indicate that a scenario is imminent?	Risk is analyzed by the red team, based in part on the metrics identified and the data collected relative to them. The team analyzes the risk of various attack scenarios of one or more modeled adversaries.
7	Conduct Mission Rehearsal Exercises (MRX)	Individually team focused notebook-like documents created with all info, ROE, resources, order of battle, objectives, desk guide, etc for each color team	OPORD/ Develop draft red team brief or white paper for SME review	Risk associated with various outcomes is assessed by the red team; a report is produced that communicates risk issues, supporting greater customer understanding of business impacts.
8	Execute mission	Findings & outcomes are documented (i.e., computed, tabulated to determine what COA implemented by teams to achieve objective based on what other teams did—Debrief	Execution/ Coordinate assessment to larger group of military experts around community	Report is consolidated into product such as VA, PPS recommendation, etc.

Table 7-1: Comparison of the Eight Standardized Red-Team Development Steps
(Pink highlights specific Red-Team Actions)

If they were not before, recent overseas operations and Presidential directives towards nation building have forced military organizations and intelligence agencies to take culture and specifically non-Western rules, assumptions, rhythms, and habits as analytical inputs to deriving context, meaning, and predictive assessments. Formal

training of red-team analysts consists of thinking tools such as alternative analysis, assumption identification exercises, and culture analysis approach procedures to force analysts to think through a more culturally informed and structured model. Have agencies and military organizations been using red-team outputs to define a way forward? By their nature, red teams define a conflict between red and blue; but how are red teams validated for their ability to capture adversary behavior?

Can red teams be made robust enough to critically simulate adversaries and others far outside Western (blue team) cultural, behavioral modus operandi in the contexts of their environments? Red-team problem sets are now based on encountering tribal and non-state red teams. Green, pink, and white teams have been added to account for non combatants, coalition, or neutral parties to capture complexities that standard binary red-blue simulations cannot capture. Do red offer valid methodologies to assess risk, define capabilities, identify gaps, and determine opportunities to American operational elements? It appears that due to the need to anticipate and mitigate surprise in the context of resource limitations, governmental organizations are seeking out formulas and approaches that enhance the ability of decisionmakers to systematically manage risk, account for probable (not any and all) adversaries, and reasonably protect assets.

Since the study was a descriptive analysis using a case-study methodology to identify the processes four organizations use to design, implement and ensure non-Western red-team realism in their war-gaming exercises, the data collection used grounded theory which identified the methods, tools, processes, personnel, and practices the four organizations used to develop their red teams.

RT Hypothesis Subject Area	UFMCS	ONI/DET	JIOC/DIOCC	SNL-NISAC
Doctrine, governance structure, operating guidelines, diffused or coalesced management structure	Some but accepts existing Command structure, products, and role is defined by leadership (Weakness)	Yes, can address doctrine and governance issues in red team	Some doctrine red teaming but similar to UFMCS in that what is in place is accepted and worked with	Some influence, but the lab accepts the governance as another element of the physical protection system to be evaluated
Weapons/operating/information system hardware, facility, bases	Some, but the embedded red team usually works with existing orders of battle or the introduction of one realistic element into the AOR	Yes, a strength of the red team	Some but the focus is on intelligence, surveillance, and reconnaissance for the COCOM	Yes, this is a strength because every base element is systematically captured for overall assessment
Strategy, operational approach, tactics	Yes, this is a primary strength of the UFMCS red team)	Yes, a strength of the red team	Yes, this is a strength for the DIOCC/JIOC approach	Yes, existing and proposed strategies are evaluated against one another
Conventional &/or standard analytic approach, methodologies, tools, procedures, processes, etc.	Yes, analytic approaches are emphasized at UFMCS	Yes but cannot account for non-state adversaries	Yes, this is another strength for the red team	Yes, this is a strength of the NISAC approach because the attributes of the PPS are quantified via methodology
People, staff, human characteristics, level of training, expertise, & knowledge/skills/abilities	There is some but reach back is something that is valued and very necessary especially when forward deployed	Some, but this appears to be a weakness if the red team designers cannot get access to specific expertise	Some, but only if there is reach back via a community of red team and academic experts via social networks	Some, however, the NISAC approach cannot quantify all variables outside the analysis such as some psychological or religious extremism
Organizational structure, order of battle, or alignment/mix of forces or security	Yes, that is another strength of the UFMCS approach	Yes, that is a strength of the ONI/DET approach	Yes, very similar to UFMCS	Yes, this is a primary output of the PPS

Table 7-2: Red-Team Applications Across The Case Studies

7.2 Interview with Joint Chiefs of Staff (Chief's) Action Group (CAG)

In an interview with the Joint Chiefs of Staff (JCS) Chairman's Action Group (CAG) staff O-6 (Colonel and Navy Captain ranks), a series of questions was asked about red teams and what methods JCS and other decisionmakers are using to evaluate their effectiveness in United States military and intelligence communities. The Secretary of Defense and the CAG staff believes they are a great way to avoid groupthink, validate planning decisionmaking, and are a good investment.[249] On the issue of some COCOMs having robust well-developed red-team elements that develop a multitude of products and some COCOMs having not yet defined their concept of operations much

less having an actual red team, the CAG staff believes they are here to stay as long as the current Chairman (Admiral Michael Mullen) wants to engage in the approach. Other COCOMs will need to step up and develop the capability the next chairman may not find red teams so useful and the CAG staff will adapt to new methods and approaches with new personnel and new resources according to the CAG staff. On the disparities between COCOMs adopting JIOCs, the CAG staff admitted that some were ahead of others; i.e., COCOM *X* has very dynamic and aggressive J-2 leadership that was on the leading edge of what the capability brings to the command. In fact this COCOM Vice Admiral in charge of the COCOM joint intelligence office and study respondent was posting red-team analytical products on the Joint Worldwide Intelligence Communication System (JWICS) Intelink (*Intellipedia* for intelligence analysts) before other COCOMs had fully identified the requirement for a red team within their decisionmaking staff.

The CAG staff agreed there are two main red-team "poles;" *Threat emulation* and *decision support*. See Figure (7-3).[250] The CAG staff also stated that there is a real need for red-team TTPs, cookbooks, systematic methodologies, and standards but that those will come because we have very capable private industry and government organizations working such issues.[251] As for instances whereby operational plans were changed in Afghanistan and Iraq due to red-team findings/outputs/recommendations, the JCS Staff said this was happening every day and had increased combat effectiveness and resulted in increased mission success.[252]

In the aforementioned operations, the CAG Staff stated that red-team findings, outputs, and recommendations have resulted in increased mission success (i.e., saving American/Coalition lives, increased enemy deaths, provided for new efficiencies/effectiveness, and increased gained "familiarity" or expertise) by refocusing coalition efforts; refining approaches. However, the CAG Staff cautioned that change is never as agile nor as fast as Admiral Mullen desires it to be. There are still immense difficulties to contend with given the mission, existing constraints in theatre, and the fundamental objectives of the national decisionmakers.[253]

In a discussion of whether or not red-team insertion into COCOMs had an effect on general staff decisionmaking yet results in documented increases in understanding the adversary, the data is mixed. The CAG staff has seen more definition and understanding of threat nodes and networks, centers of gravity, asymmetric/non-linear warfare, new theories of understanding Non-Western strategies, operational approaches, tactics, doctrine, and behaviors; but there is much that is not captured. The Joint Chiefs of Staff believe the insertion of red teams at the command level will result in more outreach to tribal elements and provided for what the DoD calls "human terrain" analysis. This has resulted in more success in OIF (Now called Operation Iraqi Dawn) and a better understanding of organizational networks, cells, virtual groups, and tribal elements.

7.3 Red-Team Issues

Based on the study, there appear to be a number of unresolved issues with red teams and red-teaming such as --if they are so great why are they not being institutionalized more rapidly? First and foremost, the definition of red teams and red-teaming is interesting but in actuality only a subset of *adversary analysis*. Adversary analysis can include a number of analytical tools listed in Table (5-3) that listed a number of tools, techniques, and procedures; or the very wide DSB definition of red-teaming to include surrogate adversaries/competitors, devil's advocates, and advisory boards that red-team developers may call red-team approaches, but are more encompassing and may be analytical approaches that are labeled red teams but are much more. The concept of red-teaming only opens the door to a number of very interesting adversary analytics, critical thinking exercises, and adversary thought/worldview[254] analysis methodologies but may be limiting the discussion to only threat emulation-type *red-teaming* analysis to organizational leadership or decisionmakers unfamiliar with more robust or unconventional approaches.

Another issue is the red-team outputs and products. The main reason they are not widely disseminated is because they may depict fatal vulnerabilities or are "owned" by the sponsor who paid for them. As discussed in earlier introductory sections, few organizations are enthusiastic about sharing their shortcomings, vulnerabilities, weaknesses, or methods for compromising their systems.

Finally, the last issue is simply one of time and resources. Few organizations have the extra resources to invest in red teams that expose their shortcomings, lack of planning, poor risk mitigation, and inability to factor in an adversary's complex or simple courses of action that circumvent an organization's proud investments in doctrine, systems, and equipment. Red teams and adversary analysis groups must maintain a distinct separation and cutting edge distance from the normal organizational cultures, values, and norms. By doing that, they are outsiders and not accepted by all parental organizational elements. Once they gain acceptance, they almost always lose their separation and distinct views that may have allowed them the red-team success in the first place. The red team's acceptance by the organization may actually sow the seeds of their demise.

7.4 Red-Team Schools of Thought

Red-teaming may borrow from a number of other analytic approaches, tools, and methodologies depending on the emphasis, blue-team needs, and most importantly, whether the red team has a threat emulation or decision support emphasis. Within the micro analytic red-team methodology, there are a number of schools of thought. The CIA Kent Center red-team model focuses on modeling and emulation of individual or groups to forecast possible intentions or actions. The center is supported by in-depth technical knowledge subject matter experts (SMEs) or Human Intelligence (HUMINT) reporting on the entity being modeled. It is often conducted as a facilitated "team" effort, but is also conducted at the analyst level depending on the target.[255]

Information Operations/Cyber red teams perform vulnerability assessment techniques designed to identify network/information system weaknesses. Similar to the SNL Defense Systems Agency model identified in Section 5, they often employ known or suspected adversary tools and techniques, and also employ forecasted or potential adversary capabilities. They can focus on defense, counter-intelligence (internal), or offensive red teams. Similarly, the physical security red team is another vulnerability assessment or security testing technique whereby a "modeled" adversary attempts surveillance, reconnaissance, attack, or other COAs.[256] This is exactly the NISAC approach from Section 6.6.

Opposing Force (OPFOR) red teams are used in war games, training or exercises, an effort to apply adversary capabilities and tactics to achieve a "realistic" exercise while also achieving training objectives.[257] Sometimes referred to as "Red Cell," these red teams are generally threat emulation approaches that rely on a group of subject matter experts who have substantial understanding of adversary military weaponry, doctrine, and capabilities and are extremely capable in understanding Russian, Chinese, Iranian, DPRK, or other possible adversary force but do not take on OPFOR roles outside those state actors.

Alternative analysis red teams are rigorous, critical assessment of hypotheses, assumptions, evidence, applied logic, assertions and conclusions in intelligence analysis products. These red teams are closest to the cadres of decision support personnel TRADOC's UFMCS is currently training at Fort Leavenworth. These analysts are being embedded in COCOM and DIOCC intelligence organizations to perform structured analytic techniques including Devil's Advocacy, Analysis of Competing Hypotheses, etc. on strategy documents, procedures, policies, and other outputs of the Command planning process.

Red cell red teams are independent, thought-provoking, often contrarian "*What If*?" analysis designed to challenge "conventional wisdom" or mainline intelligence views.[258] Speculative, overtly non-authoritative, and often not based on intelligence sources, but

intended to be plausible, these red teams are not bound by reality and were first instituted by Director of National Intelligence (DCI) George Tenet after the 2003 invasion of Iraq (*Operation Iraqi Freedom)* found very few weapons of mass destruction. These red teams are often considered an element of Alternative Analysis red teams but have no set role in operational decisionmaking. They are admittedly a pet project of the DCI.

According to DIOCC/JIOC proponent Cordray (2007), there are a number of red-team schools of thought see Table (7-3) below.

RED TEAM *SCHOOLS*[259]	STRENGTHS	WEAKNESSES
CIA Kent Center –Modeling and emulation of an individual or group to forecast possible intentions or actions.	In-depth understanding allows great ability to get beyond rhetoric or appearances of entity to get at primary motivators and needs	Compartmentalized findings (especially HUMINT) are not distributed beyond "need to know" sub-community within NCS and Directorate of Intelligence. Military with only SECRET clearance are not privy to findings.
IO/Cyber –A vulnerability assessment technique designed to identify network/information system weaknesses.	Can quickly expose complex patterns of weakness or identify breakdowns invisible to outsiders	Based on multiple assumptions that may not include basic needs
Physical Security–A vulnerability assessment or security testing technique whereby a "modeled" adversary attempts surveillance, reconnaissance, attack, or other COAs. (SNL-NISAC model)	Structured assessment that can objectively break down components and identify the weakest links	Derived from algorithmic equations that may have forgot very qualitative issues or fundamental facility needs like water food, and air for personnel
Opposing Force–Used in war games, training or exercises, an effort to apply adversary capabilities and tactics to achieve a "realistic" exercise while also achieving training objectives. Similar to NWC/ONI DET model.	Findings can have breakthrough effect on strategy, doctrine, tactics For example: enemy forces are exposed for weaknesses they have despite force structure superiority	Cannot readily use non state actors prefer opposing military forces only
Alternative Analysis –Rigorous, critical assessment of hypotheses, assumptions, evidence, applied logic, assertions and conclusions in intelligence analysis products/ Approach taught at UFMCS.	Defined set of analytic tools, techniques, procedures that force cadre of experts to look at what can go wrong not advocate or champion a favored or specific course of action	Findings not easily accepted by fully vested senior leaders who have much to lose if "crazy" ideas are accepted
Red Cell –Independent, thought-provoking, often contrarian "What If?" analysis designed to challenge "conventional wisdom" or mainline intelligence views.	Used to provide opposite view of popular wisdom/course of action and speculate on entirely different reality	Very independence makes them vulnerable to bureaucratic group-think and vested entrenched leaders who find their analysis entertaining rather than actionable
Corporate –Critical, expert, and often independent peer review of organizational structures, operational processes, future plans, products and proposals in light of the business environment.	Generally private sector analytic approach whereby brought in by organizational leadership to provide senior level independent inquiry into courses of action, plans, products, lines of business	Agile proposals are easier identified than implemented by rank and file
Umbrella –Any single or a combination of practices prescribed by the schools of thought above. Basically, any rigorous staff process that provides threat emulation, alternative analytic methods, contrarian views, or critical review.	Café or al la carte red team approach that applies best set of methodologies to a particular problem set or blue issue	Meta analytic approach is expensive and impractical—danger of making "everybody" mad at findings

Table 7-3: Red-Team Approaches
(Orange represents four case studies herein)

Corporate red teams are critical, expert, and often independent peer review of organizational structures, operational processes, future plans, products and proposals in light of the business environment, assessed competitor activities, and customer preferences.[260] Their role of adversary is played as more of a competitor or as a response to a market condition. Their scenarios include conditions such as if prices of a commodity go up, what will our competitor's product do in the market; If 2020 has smaller microchips with vastly more computing power, then consumers will want what kind of portable information systems for what purposes? If China has as many honor students as America has students, what kind of products and services will these individuals be demanding?

Umbrella red teams are any single or a combination of practices prescribed by the schools of thought above. Umbrella red teams use combinations of the above red analytical schools of thought to derive meta-analytical results. Any rigorous staff red-teaming process that provides threat emulation, alternative analytic methods, contrarian views, or critical review can be called an umbrella red team. These can be employed across all disciplines including intelligence, operations, military, and economic disciplines.[261] These umbrella red teams require expertise across disciplines and are prohibitively expensive because they pull together complex adversarial relationships. They often need corporate red-team organization contracts with expert abilities to detangle possibly conflicting findings, hot wash results, compile a series of scenario outcomes, and derive findings where the participants can see only parochial interests.

The red teams schools discussed above are shown below in relation to the two red-team poles threat emulation and decision support. Figure (7-1) below places each red-team school in its binary relation to threat emulation and decision support. One can see that OPFOR and red cell red teams are much more predisposed to threat emulation and less to decision support. Whereby red-team schools such as alternative analysis and corporate red-teams' primary goal is to provide organizational leadership with perspective on an important decision or series of decisions they may be grappling with. Providing the decisionmaker with valuable proof-of-concept results or prototype a

particular course of action before the actual decision is made in the real world is the goal of umbrella and also alternative analyses red teams.

Hybrid red teams like the Kent School, those that perform physical security VAs and IO/cyber analyses (NISAC), and umbrella red teams fall in the middle because they take characteristics of each extreme. They may have some threat definitions, risk analyses, threat trees, or adversary conditions but their outputs are intended for decisionmakers as support tools—to determine where to place resources or what product line has the best chance at profitability in a given timeframe.

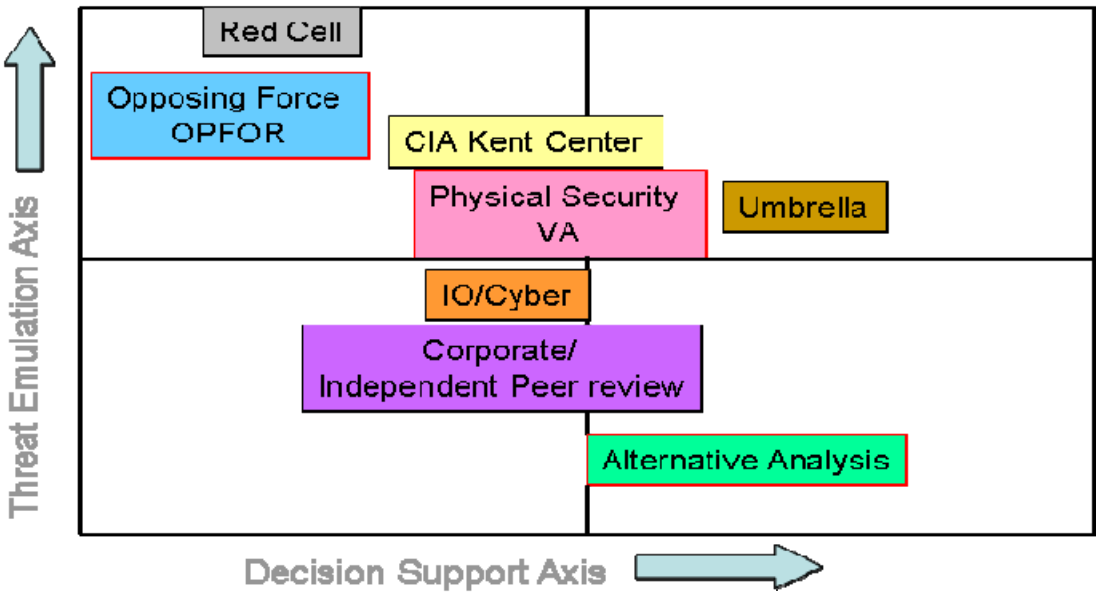


Figure 7-1: Basic Red-Team Taxonomy
(Red border represents the red-team case studies)

The results of the study provide a more complete examination by outsiders of red-teaming methodologies used by defense and national security organizations. Questions answered include: Does a method for capturing adversaries' way of thinking, planning and operating have value? The answer is *yes* and military organizations have dedicated substantial resources towards building the capability, training red teams, embedding them in operational elements like combatant commands, and giving their outputs such as analytic assessments directly to decisionmakers. Intelligence

community organizations have always done it and specifics of their programs were not selected as case studies referenced in this study.

7.5 Areas for Future Study

A key area of future red-team study is the cyberspace environment. The Sandia IORTA and IDART models may be excellent starting points for looking more closely at the growing threat of hacking into information systems. Exploitation is occurring via fraudulent accounts, insertion of malware, and other more innovative strategies. The use of red teams to capture the mindset of foreign governments and the hackers themselves could go far in identifying the hacking methods, malicious coding, and virus types used before they attack to ensure the proper level of system security elements are in place before the attack occurs.

Another area is developing red teams that immerse themselves in the culture to be red-teamed. This analytical approach would consist of literally deep diving red-teamers into a virtual world of religious, cultural, (including world view) and other attributes representing a particular adversary. The approach could have avatars or other computer-generated natives of a particular target culture interact with the red-team participants and allow them to experience stimulus material designed to produce a degree of paradigm shift and inculcate a greater understanding of the adversary's perspective which could include many non-Western traits, concepts of non-linearity, and space and time. The Institute for Defense Analysis (IDA) is developing something called "Foreign Thoughtworlds" that shows some promise. There should be a DSB commission to further examine and select alternative adversary analysis programs that are able to deep dive into cultures both *older that ours* (based on medieval mores, tribal codes of honor, and with different concepts of time and space), and *newer that ours* (with computer generated virtualization and instant global communications).

A third area of study is the concept of human terrain analysis. Some of the innovative methods now being used across the Department of Defense and intelligence community include combining historical data with geospatial analytic predictive techniques that seek to project where an event or individual can be found in the future. This technique blends the social sciences with geospatial visualization technology to predict adversary behavior. Analytic red teams that specialize in human terrain can develop models of human behavior that narrow the analytic and operational search space in areas of interest. Thuermer (2008) believes the creation of tribal polygons (the projection of where indigenous groups' contours and edges are, based on using food or watershed analysis techniques to make up for the lack of good, factual data), status group mobility signatures that depict the 'operating environment' of certain groups and likely freedom of movement for elements of those groups; and geospatial pattern matching (the comparison of individual geospatial patterns to group patterns to assess membership in certain groups) [262] and other similar methods can be used to validate and assess red teams based on tribal decisionmaking This is one example of how red-team analytic techniques can be fused with the social sciences and intelligence to improve the kind of analysis needed in failed states or areas with strong tribal bonds going back thousands of years.

Red-Teaming Studies and Analyses Literature

Addington, Larry H., Patterns of War Since the Eighteenth Century, Washington DC: Indiana University Press, 1994.

Barnett, J. W., Insight into Foreign Thoughtworlds for National Security Decisionmakers, Institute for Defense Analysis, IDA document D-2665, Log H 01-002007.

Beckerman, Linda, Non Linear Dynamics of War, McLean, VA: unpublished paper, SAIC, 2005.

Brown, Michael, Andrew May, and Matthew Slater, Defeat Mechanisms: Military Organizations as Complex Adaptive Nonlinear Systems, Final Report for the Office of Net Assessment, Office of the Secretary of Defense; Strategic Assessment Center, SAIC, 2000.

Coram, Robert, Boyd: The Fighter Pilot Who Changed The Art of War, New York: Little, Brown, and Co., 2004, p 2.

Cowan, Jeffrey L.,Warfighting Brought to You By…, Proceedings, US Naval Institute, USMC Essay Writing Contest award Winner, discussing U.S. Air Force on John Boyd's influence on US Marines war fighting doctrine, June 1997.

Defense Science Board, Task Force on the Role and Status of DoD Red-team Activities, Office of the Undersecretary of Defense for A,T&L, Sep. 2003.

Gordon, Theodore J., Frontiers of the Future: Madmen, Methods, and Massive Change, National Intelligence Commission discussion paper, 2005.

Grey, Wilbur, Adapted from the author's master's thesis Playing War: the Applicability of Commercial Conflict Simulations to Military Intelligence Training and Education (DIA Joint Military Intelligence College, Bolling AFB, DC, 1995).

Hammonds, Grant T., and The Mind of War: John Boyd and American Security, Washington DC: Smithsonian Press, 2001.

Halasz, Laslo, Literary Discourse: Aspects of Cognitive and Social Psychological Approaches, Berlin: De Gruyter, 1987.

Jenkins, Brian Michael, The Operational Code of the Jihadists, A Briefing Prepared for the Army Science Board, Rand Corporation, unpublished paper, April 1, 2004.

Jenkins, Brian Michael, Looking at al Qaeda from the Inside Out, Defense Adaptive Red-team (DART) an annotated briefing, #03-4, Hicks and Associates, December 2003.

Kelly, Jack, Little Known Pilot Shapes Iraq War, Pittsburgh Post-Gazette, March 21, 2003.

Lind, William S., The Three Levels of War, unpublished blog, Free Congress Foundation, 2003.

Malone, Timothy, and Reagan Schaupp, The "Red-team" Forging a Well-Conceived Contingency Plan, in Aerospace Power Journal Summer 2002, p 1-3.

Mateski, Mark, Red-team Journal Method Paper 3.03, p 1, 2004

McGannon, Michael, Developing Red-team Tactics, Techniques, and Procedures/ Method Paper 1.04, in Methods, Red-team Journal, downloaded June 2004, p 1.

Morgan, Gareth. Images of Organization. Newbury Park: Sage Publications, 1996.

Murdock, Clark A., The Role of Red-teaming in Defense Planning, Defense Adaptive Red-team (DART) working paper #03-3, Hicks and Associates, August 2003.

Murray, Williamson, Experimentation in the Period Between the Two World Wars: Lessons for the 21st Century, IDA Document D-2502, October 2000.

Murray, Williamson, Red-teaming: It's Contribution to Past Military Effectiveness, Defense Adaptive Red-team (DART) working paper #02-2, Hicks and Associates, Sep. 2002.

Murray, Williamson, Thoughts on Red-teaming, Defense Adaptive Red-team (DART) working paper #03-2, Hicks and Associates, May 2003.

Perrow, Charles, Complex Organizations: A Critical Essay, Glenview, IL: Scott, Foresman & Co., 1972.

Sanders, T. Irene and Judith McCabe, The Use of Complexity Science: A Survey of Federal Departments, Agencies, Private Foundations, Universities, and Independent Educational and Research Centers, Report to the U.S. Department of Education, Oct. 2003.

Sandoz, John F., Red-teaming: A Means for Transformation, IDA Paper P-3580, January 2001

Whitley, John and Judy Moore, Red-teaming and the Hypothesizer Concept, Sandia National Laboratories, downloaded from DoD website 2004.

Woodaman, Ronald F. A., Agent-Based Simulation of Military Operations Other Than War (MOOTW): Small Unit Combat, Naval Postgraduate School, unpublished paper, 2000.

Cultural Comparisons and Contrasts Between East and Occidental Literature

Barnett, J. W., Insight into Foreign Thoughtworlds for National Security Decisionmakers, Institute for Defense Analysis, IDA document D-2665, 2005.

Benyamin, Naphtali, Arab Way of War: Culture, Militant Warfare, and the Raiding Strategy, MSSI Thesis DIA unpublished, 2005

Biddle, Stephen, and Stephen Long, Democracy and Military Effectiveness: A Deeper Look, Journal of Conflict Resolution, Vol. 48, no. 4, 2004

Borschein, Joseph, Counterterrorism and Military Operations Other Than War (MOOTW) in the Middle East: New Lessons from Lebanon and Somalia, MSSI Thesis, Defense Intelligence Agency-unpublished paper, 2005

Celibi, Evliya, Seyahatname (Istanbul:1928), vol . VII, pp 318-319: German translation by R.F. Kreutel, Im Reiche des goldenen Apfels (Graz:1957☺ as referenced by Lewis in What Went Wrong: The Clash Between Islam and Modernity in the Middle East, Lewis, Bernard, Lewis, Bernard, What Went Wrong: The Clash Between Islam and Modernity in the Middle East, p. 64-65.

Clay, Joy A., Congressional Hearings: Neglected as an Administrative Process, unpublished manuscript, 1989

Coram, Robert, in on line review of Boyd: The Fighter Pilot Who Changed The Art of War, 2004.

Derne, Steve, Cultural Conceptions of Human Motivation in The Sociology of Culture, ed. Diana Crane (Cambridge: Blackwell Publishers, 1994

Dialdin, Dania, and James Wall in Third Parties and Culture, Negotiation Journal, October 1999

JCS Joint Publication 3-07.3 Joint Tactics, Techniques, and Procedures for Peace Operations([Washington, DC:GPO], 12 February 1999) IV-2.

Hammonds, Grant, downloaded from Fast Company.com website Review of John Boyd, Fast Company.com, 2002, Issue 59, 2004, p 1.
Hatti Efendi, Mustafa, Viyana Sefaretnamesi, ed. Ali Ibrahim Savas (Ankara:1999)

Huntington, Samuel P., The Clash of Civilizations and the Remaking of World Order, Simon and Shuster, New York, 1996

Izzi, Tarib-i Izzi (Istanbul: 1199/1784), p190 ff as referenced by Lewis in What Went Wrong: The Clash Between Islam and Modernity in the Middle East

Jenkins, Brian M., The Operational Code of the Jihadists, Rand Corporation, Briefing presented to the Army Science Board, April 1, 2004

Kelly, Jack, Little Known Pilot Shapes Iraq War, Pittsburgh Post-Gazette, March 21, 2003.

Kuhn, Thomas S.,The Structure of Scientific Revolutions, Univ. of Chicago Press, 1962, Chicago

Lewis, Bernard, What Went Wrong: The Clash Between Islam and Modernity in the Middle East, Oxford University Press/Perennial, New York, 2002

McCormick, Gordon H., Terrorist Decisionmaking, Annual Review of Political Science Vol. 6, June 2003, p 3.

Miller, Julie, Culture and Intelligence Analysis: The American Reception of Arab Cultural Norms, Masters of Strategic Intelligence Thesis, Joint Military Intelligence College, 2003

Mintz, John and Douglas Farah, In Search of Friends Among the Foes: The World After 9/11, Washington Post September 11, 2004.

Sabatier, Paul A., Theories of the Policy Process, In Theoretical Lenses on Public Policy, Westview Press 1999

Sayyid Qutb, Milestones, downloaded from website IJTIHAD [http://www.ijtihad.org/sq.htm], taken from an executive summary by M. A. Muqtedar Khan

Smith, S. Douglas, Naval War College book review on The Age of Sacred Terror, Proceedings 2004.

Strauss, Anselm, and Juliet Corbin, Grounded Theory Methodology: An Overview, in Strategies of Inquiry, Norman K. Denzin and Yvonna S. Lincoln, Sage Publications, Inc., Thousand Oaks CA, 1994

Tarib-I Cevdet (Istanbul: 1309/1892), vol. IV,p 355. in Lewis's What Went Wrong: The Clash Between Islam and Modernity in the Middle East

US Army TRADOC, Arab Culture Level I Lesson Plan ISO1C13L / Version 001, 1 Nov 2005

US Army, TRADOC, Arab Culture Level II Lesson Plan ISO1C13L / Version 001, 1 Nov 2005, Module downloaded from TRADOC website.

Organizational Decisionmaking Literature

Argyris, C., & Schön, D. (1978) Organizational learning: A theory of action perspective, Reading, Mass: Addison Wesley.

Bolman, L. G. and Deal, T. E. (1997) Reframing Organizations. Artistry, choice and leadership 2e, San Francisco: Jossey-Bass. 450 pages.

Castells, M. (2001) 'Information technology and global capitalism' in W. Hutton and A. Giddens (eds.) On the Edge. Living with global capitalism, London: Vintage.

DePree, M. (1990) Leadership is an Art, New York: Dell.

Drucker, P. (1977) Management, London: Pan.

Easterby-Smith, M. and Araujo, L. 'Current debates and opportunities' in M. Easterby-Smith, L. Araujo and J. Burgoyne (eds.) Organizational Learning and the Learning Organization, London: Sage.

Edmondson, A. and Moingeon, B. (1999) 'Learning, trust and organizational change' in M. Easterby-Smith, L. Araujo and J. Burgoyne (eds.) Organizational Learning and the Learning Organization, London: Sage.

Etzioni, A. (1995) The Spirit of Community. Rights responsibilities and the communitarian agenda, London: Fontana Press.

Etzioni, A. (1997) The New Golden Rule. Community and morality in a democratic society, London: Profile Books.

Finger, M. and Brand, S. B. (1999) 'The concept of the "learning organization" applied to the transformation of the public sector' in M. Easterby-Smith, L. Araujo and J. Burgoyne (eds.) Organizational Learning and the Learning Organization, London: Sage.

Fromm, E. (1979) To Have or To Be? London: Abacus.

Guttman, A. and Thompson, D. (1996) Democracy and Disagreement, Cambridge, Mass.: Belknap Press.

Hutton, W. (1995) The State We're In, London: Jonathan Cape.

Klein, N. (2001) No Logo, London: Flamingo.

Leadbeater, C. (2000) Living on Thin Air. The new economy, London: Penguin.

Van Maurik, J. (2001) Writers on Leadership, London: Penguin.

Sabatier, Paul A., Theories of the Policy Process, In Theoretical Lenses on Public Policy, Westview Press 1999

Kuhn, Thomas S., The Structure of Scientific Revolutions, Univ. of Chicago Press, 1962, Chicago

Strauss, Anselm, and Juliet Corbin, Grounded Theory Methodology: An Overview, in Strategies of Inquiry, Norman K. Denzin and Yvonna S. Lincoln, Sage Publications, Inc., Thousand Oaks CA, 1994

Senge, P. M. (1990) The Fifth Discipline. The art and practice of the learning organization, London: Random House. 424 + viii pages. A seminal and highly readable book in which Senge sets out the five 'competent technologies' that build and sustain learning organizations. His emphasis on systems thinking as the fifth, and cornerstone discipline allows him to develop a more holistic appreciation of organization (and the lives of people associated with them).

O'Neill, J. (1995) 'On schools as learning organizations. An interview with Peter Senge' Educational Leadership, 52(7) http://www.ascd.org/readingroom/edlead/9504/oneil.html

Schultz, J. R. (1999) 'Peter Senge: Master of change' Executive Update Online, http://www.gwsae.org/ExecutiveUpdate/1999/June_July/CoverStory2.htm

Senge, P. (1998) 'The Practice of Innovation', Leader to Leader 9 http://pfdf.org/leaderbooks/l2l/summer98/senge.html

Senge, P. et. al. (1994) The Fifth Discipline Fieldbook: Strategies and Tools for Building a Learning Organization

Senge, P., Kleiner, A., Roberts, C., Ross, R., Roth, G. and Smith, B. (1999) The Dance of Change: The Challenges of Sustaining Momentum in Learning Organizations, New York: Doubleday/Currency).

Senge, P., Cambron-McCabe, N. Lucas, T., Smith, B., Dutton, J. and Kleiner, A. (2000) Schools That Learn. A Fifth Discipline Fieldbook for Educators, Parents, and Everyone Who Cares About Education, New York: Doubleday/Currency

Sennett, R. (1998) The Corrosion of Character. The personal consequences of work in the new capitalism, New York: Norton

Abelson, R.P., & Levi, A. (1985). Decisionmaking and decision theory. In G. Lindzey & E. Aronson (Eds.), The Handbook of Social Psychology, (3rd ed., Vol. 1), NY: Random House, pp. 231-309.

Hogarth, R. M. and M. W. Reder (1986). Perspectives from Economics and Psychology, in R. Hogarth and M. Reder (eds.), Rational Choice University of Chicago Press, London.

Langley A., Mintzberg H., Pitcher P., Posada E. and Saint-Macary J. (1995) Opening Up Decisionmaking: the view from the black stool, Organization Science, 6(3): 260-279.

March, J. G. (1997). Understanding How Decisions Happen in Organisations', in Z. Shapira (ed.)

Shapira, Z. (ed.) (1997). Organisational Decisionmaking Cambridge University Press: Cambridge.

Simon, H. A. (1983). Models of Bounded Rationality. MIT Press: MA.
Tversky, A. and D. Kahnemann (1981). The Framing of Decisions and the Psychology of Choice, Science 211, 453–458.
Zey M. (Ed) (1992) Decisionmaking: alternatives to rational choice models, Sage, London.

Herr, P.M. (1986). Consequences of priming: Judgment and behavior. Journal of Personality and Social Psychology, 51, 1106-1115.

McGill, A.L. (1989). Context effects in judgments of causation. Journal of Personality and Social Psychology, 57, 189-200.

Payne, J. W. (1976). Task Complexity and Contingent Processing in Decisionmaking: An Information Search and Protocol Analysis', Organizational Behavior and Human Performance 16, 366–387.

Rettinger, D. A. and R. Hastie (2001). Content Effects on Decisionmaking', Organisational Behaviour and Decision Processes 85(2), 336–359.

Tversky, A. and D. Kahnemann (1986). Rational Choice and the Framing of Decisions, in R. Hogarth and M. Reder (eds.), Rational Choice University of Chicago Press, London.

Zalesny, M.D., & Ford, K. (1990). Extending the social information processing perspective: New links to attitudes, behaviors, and perceptions. Organizational Behavior and Human Decision Processes, 47, 205-246.

Jungerman, H. (1983). The two camps on rationality. In R.W. Scholz (Ed.), Decisionmaking under uncertainty, (pp. 63-86). Amsterdam: Elsevier.

Funder, D.C. (1987). Errors and mistakes: Evaluating the accuracy of social judgment. Psychological Bulletin, 101, 75-90.

Kahneman, D. (1991). Judgment and decisionmaking: A personal view. Psychological Science, 2, 141-145.

Wilson, T.D., & Schooler, J.W. (1991). Thinking too much: Introspection can reduce the quality of preferences and decisions. Journal of Personality and Social Psychology, 60, 181-192.

Terrorism and Political Violence Literature

Alexander, Yonah, and John M. Gleason, Behavioral and Quantitative Perspectives on Terrorism, New York: Pergammon, 1981.

Anonymous (Michael Scheuer), Through the Eyes of Our Enemies, Washington DC: Brasseys, 2003.

Arquilla, John and David Ronfeldt, Networks and Netwars, Santa Monica: Rand, 2001.

Benjamin, David, and Steven Simon, The Age of Sacred Terror, New York: Random House, 2003.

Crenshaw, Martha, The Logic of Terrorism: Terrorist Behavior as a Product of Strategic Choice*, in Origins of Terrorism,* Edited by Walter Reich, Washington DC: Woodrow Wilson Center Press, 1990, p. 7-9.

Flower, Elizabeth, The Elements of the World's Religions, Shaftesbury, Dorset: Element Books, 1997.

Garrett, Eric, Why Radical Islam Might Defeat the West, Asia Times on line, Oct. 22, 2004.

Hoffman, Bruce, Inside Terrorism, New York: Columbia University Press, 1998.

Howard, Lawrence, Terrorism: Roots, Impacts, Responses, New York: Praeger, 1992.

Jenkins, Brian M., The Operational Code of the Jihadists, Rand Corporation, Briefing presented to the Army Science Board, April 1, 2004.

Laqueur, Walter, The New Terrorism: Fanaticism and the Arms of Mass Destruction, New York: Oxford University Press, 1999.

Lewis, William H., The Growing Reach of Radical Islam, Joint Forces Quarterly, Autumn 1995.

Loescher, Michael, Proteus: Insights from 2020, (compiled by Pamela Krause), Exercise conducted by national Reconnaissance Office (NRO) for Directorate of Imagery Analysis and Acquisition (IMINT), Washington DC: Tasc Corp., Deloitte Consulting and Copernicus Press, 1998.

MacKerrow, Edward P., Understanding Why: Dissecting Radical Islamicist Terrorism with Agent Based Simulation, Los Alamos Science, Number 28, 2003.

McCormick, Gordon H., Terrorist Decisionmaking, Annual Review of Political Science Vol. 6, June 2003, p 3.

Miller, James A., Terrorism Open Source Intelligence Reports (TOSIRs) #1-195+ September 2001-February 2005, Interaction Systems Incorporated for the Central Intelligence Agency.

Miller, James A., Regional and Country Watch List (RCWL) #1-45+ November 2003-February 2005, Interaction Systems Incorporated for the Central Intelligence Agency.

Miller, James A., Warning and Intelligence on the Internet Review (WIIR) #1-104+ October 2002-February 2005, Interaction Systems Incorporated for the Central Intelligence Agency.

Pipes, Daniel, The Western Mind of Radical Islam, First Things/Journal of Religion, Culture, and Public Life, Dec. 1995.

Post, Jerrold, Terrorist Psycho-Logic: Terrorist Behavior as a Product of Psychological Forces*, in Origins of Terrorism*, Edited by Walter Reich, Washington DC: Woodrow Wilson Center, 1990, p. 25-29.

Qutb, Sayyid Qutb, Milestones, Courtesy of IJTIHAD [http://www.ijtihad.org/sq.htm], executive summary by M. A. Muqtedar Khan, downloaded from internet June, 2004

Reich, Walter, Origins of Terrorism, Washington DC: Woodrow Wilson Center, 1990.

Reich, Walter, Understanding Terrorist Behavior: The Limits and Opportunities of Psychological Inquiry, in Origins of Terrorism, Washington DC: Woodrow Wilson Center 1990, p 261.

Spencer, Robert, Whitewashing Radical Islam, Front Page Magazine, Sep. 3, 2003.

Footnotes

[1] Ibid., downloaded from wargaming discussion on analytics 9/08.
[2] US Army derived excerpt on scenarios from internet search 7/08.
[3] Ibid., excerpt on modeling and simulation from internet search 7/08.
[4] Ibid., excerpt on types of simulations and discussion of stochastic models internet search 7/08.
[5] DRII_____
[6] Malone, Timothy, and Reagan Schaupp, The "Red team" Forging a Well-Conceived Contingency Plan, in Aerospace Power Journal Summer 2002,downloaded from internet 2004, p 1.
[7] Stanford University journal—get citation--
[8] McGannon, Michael, *Developing Red-team Tactics, Techniques, and Procedures*/ Method Paper 1.04, in Methods, Red-team Journal, downloaded June 2004, p 1.
[9] Malone and Schapp, Ibid., p 9.
[10] Ibid., p 9.
[11] JP 1 Doctrine for the Armed Forces of the United States, 14 May 2007, Chapter VII, page VII-6, JP1.
[12] Ibid., p 3.
[13] 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, DC, pp 2-4.
[9] Malone, Timothy, and Reagan Schaupp, The "Red team" Forging a Well-Conceived Contingency Plan, in Aerospace Power Journal Summer 2002,downloaded from internet 2004, p 1-3.
[15] Definition downloaded from http://www.decision-making-confidence.com/rational-decision-making-models.html of 1/11/10. p 1.
[16] Robbins, Stephen P., and Timothy A. Judge. Organization Behavior. 12th ed. Upper Saddle River, New Jersey: Pearson Prentice Hall, 2007. 156-158.
[17] Malone and Schaupp, p 4.
[18] Mateski, Mark, Red-team Journal Method Paper 3.03, p 1, 2004
[19] Malone and Schaupp, p. 3.
[20] DSB Red Team Task Force, p. 12.
[21] DSB Red Team Task Force, p. 15.
[22] Joint Publication (Pub) 5-00.2, Joint Task Force Planning Guidance and Procedures, figure IX-10.
[23] Ibid., figure IX.-19
[24] Malone and Schaupp, p. 4.
[25] Ibid., p. 5.
[26] Palmer, C.C., Ethical Hacking, IBM Systems Journal, 2001.
[27] Ibid., p 10.
[28] Schneider, p 4.
[29] Ibid., p 4.
[30] 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, DC, pp 2.
[31] Palmer, p. 3.
[32] Gallegos, Frederick, Red Teams: An Audit Tool, Technique and Methodology for Information Assurance, ISACA website, Volume 2, 2006, p. 2.
[33] Gallegos, Frederick, Red Teams: An Audit Tool, Technique and Methodology for Information Assurance, ISACA website, Volume 2, 2006, p. 2.
[34] DSB Red Team Task Force, p 9.
[35] Gallegos, p. 5.
[36] Op. cit., Department of Defense taken from Gallegos , p. 5.
[37] Gallegos, p. 6.
[38] Duggan, David p., Robert L. Hutchinson, Red Teaming 101, Sandia National Laboratories, 17 July 2004, www.cs.nmt.edu/%7Ecs491_02/RedTeaming-4hr.pdf
[39] Sparta Information System Security Organization, http://www.isso.sparta.com/documents/ia_program.pdf

[40] Information System Audit and Control Association (ISACA) web page for educators and students, http://www.isaca.org/template.cfm?section=home
[41] van der Walt, Charles, *Assessing Internet Security Risk, Part 5: Custom Web Applications Continued* Security Focus.com, web article, 2002-10-08, downloaded February 2010, p.1.
[42] Seltzer, Larry, p 1.
[43] Gallegos, p. 5.
[44] Ibid., p. 5.
[45] Amezana Technologies, Ltd., Creating Secure Systems Through Attack Modeling, 10 June 2003, www.amezana.com/downloads/docs/5StepAttackTree_WP.pdf.
[46] Ibid., p. 6.
[47] Ibid., p.2.
[48] Security Analysis and Risk Management Association (SARMA) website, discussion on Sandia National Laboratories Information Operations Red Team and Assessments, downloaded 12, December 2009.
[49] Sandia National Laboratories, web page text from website downloaded January 2009.
[50] Sandia, Ibid., p.1.
[51] http://idart.sandia.gov/methodology/Adversary_Modeling.html, used with permission for educational purposes associated with 2010 dissertation. Any additional materials (press releases and other documents) would require additional permissions, at no time shall the images be used in a document that implies any endorsement by Sandia of any point of view, product or service by Stephanie Holinka, Media Relations & Communications, Sandia National Laboratories, April 2009.
[52] Seltzer, Larry, eWeek interview with Sandia National Laboratories' Michael Skorch, 2006, p. 7.
[53] http://idardt.sandia.gov/methodology/Adversary_modeling.html, website downloaded February 2010, used with permission for educational purposes associated with 2010 dissertation. Any additional materials (press releases and other documents) would require additional permissions, at no time shall the images be used in a document that implies any endorsement by Sandia of any point of view, product or service by Stephanie Holinka, Media Relations & Communications, Sandia National Laboratories, April 2009.
[54] Seltzer, p. 8.
[55] Sandia National Laboratories website, used with permission for educational purposes associated with 2010 dissertation. Any additional materials (press releases and other documents) would require additional permissions, at no time shall the images be used in a document that implies any endorsement by Sandia of any point of view, product or service by Stephanie Holinka, Media Relations & Communications, Sandia National Laboratories. April 2009.
[56] Gallegos, p. 4.
[57] Ibid., p 3.
[58] Ibid., p 2.
[59] JP 1 Doctrine for the Armed Forces of the United States, 14 May 2007, Chapter VII, page VII-6, JP1.
[60] Paller, Allan, SANS Institute's 2005 update of its annual 20 Most Critical Internet Security Vulnerabilities report, as stated in the U.S. Computer Emergency Readiness Team (US-CERT) and the United Kingdom's National Infrastructure Security Co-ordination Centre in announcing the new findings Nov. 22, 2005: cybercriminals focused on attacking client applications and network operating systems other than Microsoft Windows, which don't receive automatic security patches, downloaded from Federal Computer Week August 2005. (Paller is the institute's director of research)
[61] Simon, Herbert A., *A Behavioral Model of Rational Choice, in Models of Man, Social and Rational: Mathematical Essays on Rational Human Behavior in a Social Setting*, New York, Wiley, p 553.
[62] Senge, Peter., Kleiner, Art., Roberts, Charlotte., Ross, Richard., Smith, Bryan., *The Fifth Discipline, Fieldbook* New York, Currency Doubleday, and Senge, Peter., Kleiner Art., Ross, Richard., Roth, George., Smith, Bryan., *The Dance of Change*, New York, Currency Doubleday, The first of the five disciplines of organizational improvement discussion.
[63] Ibid., p 1
[64] Ibid., p 4.
[65] Ibid., p 5.
[66] Ibid., p 4
[67] Ibid., p 5.
[68] Ibid., p 5.
[69] Ibid., p 6

[70] Ibid., p 6.
[71] Mateski, Mark, Red-team Journal Method Paper 3.03, p 1, 2004
[72] Schneider, William, jr, Chairman Defense Science Board, *The Role And Status of DoD Red Teaming Activities*, September 2003, p. 7.
[73] Schneider, , p. 8.
[74] DSB, p. 11.
[75] Ibid., p. 11.
[76] Ibid., p 12.
[77] Joint Publication 1.02, TRADOC, US Army.
[78] Malone, Timothy, and Reagan Schaupp, The "Red Team" Forging a Well-Conceived Contingency Plan, in Aerospace Power Journal Summer 2002,downloaded from internet 2004, p 1-3
[79] Schneider, p 9.
[80] Schneider, p. 12.
[81] Ibid., p. 8.
[82] Ibid., p. 9.
[83] Ibid., p 9.
[84] Malone, Timothy, and Reagan Schaupp, The "Red team" Forging a Well-Conceived Contingency Plan, in Aerospace Power Journal Summer 2002,downloaded from internet 2004, p 1-3.
[8] McGannon, Red team Journal, Method Paper 1.04, p 1, 2004
Ibid., Malone and Schaup, p.
[85] Ibid., p 11.
[86] Ibid., p 9.
[87] Ibid., p 9.
[88] Ibid., p 13.
[89] DSB, p14.
[90] Shanker, Thomas, *Iran Encounter Grimly Echoes '02 War Game*, New York Times, 12 January 2008, web page download.
[91] Rickerman, Maj. Leonard D., Effects Based Operations: A New Way of Thinking and Fighting, School of Advanced Military Studies United States Army Command and General Staff College, Ft. Leavenworth, KA, First Team AY 02-03, p.26-29.
[92] Ibid., p. 30.
[93] Darken, Rudy and CDR Joseph Sullivan, *Virtual Team Environments*, Naval Postgraduate School, Research October 2002, Vol 12, Num.3. p 1-9.
[94] Malone and Schaupp, p 1-3.
[95] Wilkes, p 2.
[96] Wilkes, Col. Bobby, Document created: 6 December 01, Published *Aerospace Power Journal* – Winter 2001, p 2.
[97] Malone and Schaupp, p 4.
[98] Gallegos, p. 5.
[99] Ibid., p. 5.
[100] Ibid., p 6.
[101] Clay, Joy A., Congressional Hearings: Neglected as an Administrative Process, unpublished manuscript, 1989. p
[102] Strauss, Anselm, and Juliet Corbin, *Grounded Theory Methodology: An Overview*, in *Strategies of Inquiry*, Norman K. Denzin and Yvonna S. Lincoln, Sage Publications, Inc., Thousand Oaks CA, 1994, p273-274.
[103] Dunn, _____p ?
[103] USMC CAOCL website, downloaded 2008.
[103] Ibid., website.
[104] Benson, Kevin, from Security Studies Program Seminar , Military Adaptation of Red Teaming , UFM&CS, webpage,
November 14, 2007.
[105] US Army 2009 Posture Statement signed by George W. Casey, US Army General Chief of Staff and Secretary of the Army Pete Geren, Information Paper on *Changing the Culture*, page 1, downloaded August 20, 2009.
[106] Ibid., Information Paper, page 1.
[107] DOD Dictionary, Joint Publication 1-02, available at JDEIS.
[108] US Navy , Naval Warfare College website introduction to NWC, downloaded 19 August, 2009, p.1

[109] Official U.S. Navy Web Site: Naval War College, downloaded on 20 August 2009. www.navy.mil | www.navy.com
[110] Ibid., p 2
[111] US Naval War College website, downloaded June 2009.
[112] Sandia laboratories, website at www.sandia.gov/.
[113] Selzer, Larry, Sandia's Red Teams: On The Hunt for Security Holes, eWeek.com, 2008., p. 3.
[114] Download on 22 November 2009 from http://www.sandia.gov/mission/homeland/programs/critical/nisac.html
[115] Ibid., NISAC website.
[116] Base on UFMCS discussion with red team SME respondents who wanted their students to gain the trust of the commands so that their analytical approaches would be better understood by the COCOM leadership.
[117] Compilation of primary blue team categories from DSB, (2004), UFMCS, ONI/DET, and JIOC/DIOCC, multiple pages.
[118] Ibid., p 2
[119] Ibid., p 2
[120] Spade, Marcus A., UFMCS Red team announcement 23 Sep. 2005, TRADOC News Service, downloaded from TRADOC website July 2009.
[121] Ibid., TRADOC brief p.1.
[122] Ibid., TRADOC brief p.1.
[123] Zahn, Jeffrey, as quoted in Spade, TRADOC brief, 2005
[124] Spade, TRADOC brief, p. 1.
[125] US Army Field Manual 3-07, p1-23.
[126] University of Foreign Military and Cultural Studies, Red team Handbook, v4.Oct 07, p.10.
[127] Based on interviews conducted with TRADOC UFMCS red team SMEs and other personnel April-May 2009.
[128] Ibid., p 28.
[129] Based on TRADOC UFMCS documentation and interviews with red team subject matter experts April-May 2009.
[130] Based on interviews with TRADOC UFMCS government and contractor red team SME personnel April-May 2009.
[131] Ibid., p 34.
[132] This table is based on information from the UFMCS Red Team Handbook and respondent information to show where metrics can be applied to the UFMCS curriculum.
[133] Ibid., P 36.
[134] Ibid., p 41.
[135] Naval War College website introductory information downloaded 15 June 2007 pp1-2.
[136] McKenna, Gary, An Introduction to Wargaming from the Adversary Force Perspective, Office of Naval Intelligence, Detachment NWC, Research Analyst and Wargame SME, Unclassified brief provided in May 2009.
[137] Ibid., McKenna, Gary, *An Introduction to Wargaming from the Adversary Force Perspective*, Office of Naval Intelligence, Detachment Naval War College, Research Analyst & Wargame SME, UNCLASSIFIED, 2009.
[138] Ibid., p 33.
[139] Ibid., p 36, from Fontenot, Gregory, (2005), *Seeing Red: Creating a Red team Capability for the Blue Force*.
[140] Ibid., p 36, adopted from Fontenot, 2005.
[141] Ibid., p 30.
[142] Ibid., p 30.
[143] Compiled from ONI/DET respondent interview with NWC red team SME, May 2009.
[144] Ibid., p 23.
[145] Adopted from ONI/DET handouts and discussions with NWC red team expert, May 2009, graphics used with permission of author Gary L. McKenna, Intelligence Research Analyst, Office of Naval Intelligence Detachment, United States Naval War College, 686 Cushing Road, Newport, RI 02841, SIPR email: mckenna@nwc.navy.smil.mil, JWICS email: mckenng@nmic.ic.gov, (401) 841-2405.
[146] Ibid., p 23.
[147] Ibid., p 16.
[148] Perla, Peter, The Art of Wargaming, 1990, p unknown.
[149] McKenna, Gary, Ibid., referencing /adapted from USMC WARGAMING DIVISION and Hanley, John, 1991 poli sci dissertation at Yale (On Wargaming: *A Critique of Strategic Operational Gaming*) 1991.

[150] McKenna, Ibid. p 17.
[151] Ibid., p 13.
[152] Ibid., p 20.
[153] Ibid., p 22.
[154] Ibid., p 34.
[155] Ibid., p.30.
[156] Distilled from ONI/DET red team briefings and respondents, May 2009.
[157] Kibiloski, David , *Defense Intelligence Operations Coordination Center: Red team Concept of Operations (CONOPS)*, Version 0.4, Defense Intelligence Operations Coordination Center 6 December 2007, p. 7.
[158] Taken from: Keating, Timothy J., COMMANDER, COCOM X, CAMP SMITH, OCONUS, 2 April 2009. Introduction to Combatant Command p 1.
[159] Ibid., p 1.
[160] Ibid., p 19.
[161] DoD Joint Intelligence Operations Center Guidance, Mission Essential Task List (METL) under supporting task A.2.3
[162] Roth, Ray, *DIOCC Red team Update*, 28 January, 2008, DIA, p.5.
[163] COCOM red team attributes mentioned by Defense Intelligence Agency subject matter expert respondents May 2009.
[164] Kibiloski, p 9.
[165] Ibid., p 9.
[166] Ibid., p 9.
[167] Ibid., p 11.
[168] Ibid, p 12., and interviews with COCOM X respondents.
[169] McCabe, Patrick, *Red team Concept and Operations*, United States Pacific Command Joint Intelligence Operations Center (JIOC) 2009, pp 3-25.
[170] Ibid., p. 18.
[171] Illustration was provided by DIOCC/JIOC respondent; it appears to be a proposal with J-2 as a two star (Vice Admiral lower half) whereby the text notes that currently COCOM J-2 is a three star (Vice Admiral upper half)
[172] Cordray, Rob, COCOM Collaborative Analytic Red team Process, Joint Operations Intelligence Center, 21 August 2007. p 8-9.
[173] Based on interviews with COCOM X red team SME respondents and red team leaders, March 2009.
[174] 2008 JIOC red team Survey, results, p 1.
[175] Ibid., p 1.
[176] Ibid., p 1.
[177] Ibid., p 1.
[178] Ibid., p 2.
[179] Ibid., p 2.
[180] Ibid., p 2.
[181] Based on JIOC and DIA red team SME discussions and briefings and synthesized for comparison to UFMCS drivers.
[182] Kibiloski, David , p 11.
[183] Ibid., p 12.
[184] Ibid., p 9.
[185] Cordray, p 9.
[186] Ibid., p18.
[187] Ibid., p 18.
[188] Synthesized from JIOC and DIOCC red team discussion documents, briefs and red team surveys provided by red team SMEs from DIA and graduates of UFMCS who were members of COCOM J-2 organizations in March 2009.
[189] Kibiloski, p 10.
[190] Table synthesized from field notes from COCOM X red team member interviews and briefings provided by DIA red team SMEs March-April 2009.
[191] Ibid., p 10.
[192] Ibid., p 10.
[193] Pulled from interviews with DIA red team SMEs May 2009 and red team road show documents used by DIOCC.

[194] Ibid., p 18.
[195] Synthesized from interview notes from DIA, COCOM, and other red team SME respondents April-May 2009 to derive metrics from red team critical success factors.
[196] Ibid., p 14.
[197] Ibid., p 15.
[198] Ibid., p 17.
[199] Ibid., p 17.
[200] Ibid., p 17.
[201] Garcia, Mary Lynn, *Vulnerability Assessment of Physical Protection Systems*, Sandia National Laboratories, Elsevier, Amsterdam, 2006, p 65.
[202] Ibid., p 2.
[203] Ibid., p 4.
[204] Garcia, Mary Lynn, *Design and Evaluation of Physical Protection Systems*, Sandia National Laboratories, Elsevier, Amsterdam, 2001, p referenced in Ibid., p 4..
[205] Garcia in *Vulnerability Assessment of Physical Protection Systems*, p 4.
[206] Ibid., p 4.
[207] Ibid., p 4.
[208] Adventium brief presented at the Threat Metrics Workshop--"*What information helps you anticipate your adversary?*", Red team 2007, p 7.
[209] Garcia, p 5.
[210] Ibid., p 5.
[211] Ibid., p 5.
[212] Ibid., p 67.
[213] Ibid., p 66.
[214] Ibid., p 66.
[215] Ibid., p 66.
[216] Ibid., p 67.
[217] Ibid., p 67.
[218] Ibid., p 68.
[219] Ibid., p 71.
[220] Ibid., p 71.
[221] Ibid., p 72.
[222] Ibid., Based on Garcia's simple method for estimating attack from p. 72.
[223] Ibid., p 72.
[224] Ibid., p 256.
[225] Ibid., p 256.
[226] Ibid., p 256.
[227] Ibid., p 257.
[228] Ibid., p 256.
[229] Ibid., p 259.
[230] Adventium brief presented at the Threat Metrics Workshop--"*What information helps you anticipate your adversary?*", p 14.
[231] Adventium brief presented at the Threat Metrics Workshop--"*What information helps you anticipate your adversary?*", p 14.
[232] Ibid., p 17.
[233] Ibid., p 18.
[234] Garcia, p 260.
[235] Ibid., p 262.
[236] Ibid., p 262.
[237] Ibid., p 263.
[238] Ibid., p 262.
[239] Ibid., p 262
[240] Ibid., p 262.
[241] Ibid., p 262.

[242] Ibid., p 262.
[243] Ibid., p 263 & 264.
[244] Ibid., p 306.
[245] Ibid., p 308.
[246] Ibid., p 308.
[247] Adventium brief, p 19.
[248] Collins, Pam, *Vulnerability Assessments*, Brief on Sandia National Laboratories, Eastern Kentucky University October 2006, p 3.
[249] Interview with JCS Chief's Action Group (CAG) Air Force Colonel A, June 2009, conducted at Pentagon.
[250] JCS Ibid., interview notes.
[251] JCS, Ibid., interview notes.
[252] JCS, Ibid., interview notes.
[253] JCS Ibid., interview notes
[254] *Foreign thoughtworlds* is a term used by an Institute for Defense Analysis red team methodology that far surpasses pure threat emulation red teaming.
[255] Cordray, Robert, *Collaborative Analytic Red Team Processes,* Joint Intelligence Operations Center -North 21 August 2007, p 11.
[256] Cordray, p 11.
[257] Ibid., p 11.
[258] Ibid., p 11.
[259] Cordray,, p 6.
[260] Ibid., p 12.
[261] Ibid., p 12.
[262] Thuermer, Karen E., Geospatial Crystal Ball, in United States Geospatial Intelligence Forum, MGT 2008 Volume: 6 Issue: 5 (September/October) p. 1.