NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

**BUILDING A CONTINGENCY MENU:
USING CAPABILITIES-BASED PLANNING FOR
HOMELAND DEFENSE AND HOMELAND SECURITY**

by

Thomas J. Goss

March 2005

Thesis Advisor:	Paul Stockton
Second Reader:	Andy Mitchell

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** March 2005	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Building a Contingency Menu: Using Capabilities-Based Planning for Homeland Defense and Homeland Security			**5. FUNDING NUMBERS**
6. AUTHOR LTC Thomas Goss			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

A capabilities-based approach to contingency planning offers important opportunities to strengthen both Homeland Defense and Homeland Security. The Department of Defense (DOD) and the Department of Homeland Security (DHS) have already begun moving beyond traditional threat-based and scenario-based planning methodologies toward a more capabilities-based approach, but require embracing this concept more in order to counter challenges in developing contingency plans against current threats to the US Homeland. Additionally, given the critical responsibilities of state and local governments in Homeland Security, this planning approach might be applied far beyond the Federal government. This thesis examines ways that a specialized capabilities-based planning process might be applied to Homeland Defense and Homeland Security, and applies the proposed methodology to two case studies: the US Navy Component of US Northern Command and the New York City Fire Department.

14. SUBJECT TERMS Contingency planning; planning; homeland defense; homeland security; capabilities-based planning			**15. NUMBER OF PAGES** 87
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

BUILDING A CONTINGENCY MENU: USING CAPABILITIES-BASED PLANNING FOR HOMELAND DEFENSE AND HOMELAND SECURITY

Thomas J. Goss
Lieutenant Colonel, United States Army
B.S., United States Military Academy, 1987
M.A., Ohio State University, 1997
Ph.D., Ohio State University, 2001

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
March 2005

Author: Thomas J. Goss

Approved by: Dr. Paul Stockton
Thesis Advisor

Mr. Andy Mitchell
Second Reader/Co-Advisor

Professor Douglas Porch
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

A capabilities-based approach to contingency planning offers important opportunities to strengthen both Homeland Defense and Homeland Security. The Department of Defense (DOD) and the Department of Homeland Security (DHS) have already begun moving beyond traditional threat-based and scenario-based planning methodologies toward a more capabilities-based approach, but require embracing this concept more in order to counter challenges in developing contingency plans against current threats to the US Homeland. Additionally, given the critical responsibilities of state and local governments in Homeland Security, this planning approach might be applied far beyond the Federal government. This thesis examines ways that a specialized capabilities-based planning process might be applied to Homeland Defense and Homeland Security, and applies the proposed methodology to two case studies: the US Navy Component of US Northern Command and the New York City Fire Department.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank Dr. Paul Stockton for providing me the intellectual guidance and energy to complete this thesis. I would also like to thank my wife Andria and my two daughters for giving me the motivation – and the required time – to complete this effort.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION: THE VITAL TASK OF PLANNING FOR THE WORST

A capabilities-based approach to contingency planning offers important opportunities to strengthen both Homeland Defense and Homeland Security. The Department of Defense (DOD) and the Department of Homeland Security (DHS) have already begun moving beyond traditional threat-based and scenario-based planning methodologies toward a more capabilities-based approach, but require embracing this concept more in order to counter challenges in developing contingency plans against current threats to the US Homeland. Additionally, given the critical responsibilities of state and local governments in Homeland Security, this planning approach might be applied far beyond the Federal government. This thesis examines ways that a specialized capabilities-based planning process might be applied to Homeland Defense and Homeland Security, and applies the proposed methodology to two case studies: the US Navy Component of US Northern Command and the New York City Fire Department.

Because terrorist threat actors may be both cunning and adaptive, relying on surprise to overcome security measures, military and security planners must embrace a more flexible, comprehensive, and comprehendible approach to contingency planning – a method based not on threats or scenarios, but on capabilities. The process of contingency planning and resource allocation poses one of the greatest current challenges for those responsible for protecting the US Homeland because of the severity and diversity of the threats and the required timeliness of any defensive operations and security responses. The *National Strategy for Homeland Security* recognizes this by having "manage risks and allocate resources judiciously" as guiding principles and goes on to declare, "because the number of potential terrorist acts is nearly infinite, we must make difficult choices about how to allocate resources against those risks that pose the greatest danger to our homeland."[1] At this task, military and security planners have struggled to develop a comprehensive and comprehendible planning system using existing approaches of traditional threat-based planning that focus on the "who" and scenario-based planning

[1] U.S. Department of Homeland Security. *National Strategy for Homeland Security (NSHLS)*, July 2002 (Washington, DC.: US Government Printing Office, 2002), 3.

that address the "what." To present senior decision-makers with timely and effective contingency plans, planners need to transition to a more flexible and dynamic capabilities-based planning method that focuses on the "how" and can frame required capabilities and overcome uncertainty concerning the threat.

A. WHY PLANNING MATTERS

One of the main points learned during contingency planning since 9/11 is that Homeland Defense (HLD) and Homeland Security (HLS) both require a new comprehensive and comprehendible planning process.[2] For military planners, the lack of an accepted framework and vision of the threat facing the US Homeland emerged as fundamental issues during Homeland Defense planning prior to the start of the War in Iraq. During this crisis action planning, planners continually faced the same questions: "What is the threat?" and "What tasks do you need us to do?" When it was time for the resulting plan to be briefed, a new set of questions emerged: "What are you doing about threat X?" "Why do you need resource Z?" and "How did you determine that Z is enough?" These pointed questions continue as the Department of Defense adjusts its planning process to address and counter threats of asymmetric attacks on the US Homeland from both terrorist groups and hostile nation-states.[3] A similar challenge faced Homeland Security planners since 9/11 because of the fact that terrorist groups' main goal is always surprise and shock.

The traditional purpose of contingency planning is to provide information, analysis, and recommendations to senior decision-makers to assist in the vision and expression of potential courses of action to meet future crises. This paper will not address long-range budgeting and organizational planning such as military force structure and

[2] In this manner, the attacks of September 11th were not only a wake-up call to a more dangerous world, but also triggered an immediate re-thinking of responses to terrorists and terrorism. As the impressions of 9/11 and technological proliferation have changed the strategic environment, leaders and planners at every level of the government wrestled with how to meet the terrorist threat. "We cannot defend America and our friends by hoping for the best," states the current *National Security Strategy,* "so we must be prepared to defeat our enemies' plans, using the best intelligence and proceeding with deliberation." The act of "proceeding with deliberation" identifies the current organizational stumbling block for many academics, strategists, and planners who try to match plans and capabilities with perceived threats. *National Security Strategy of the United States* (Government Printing Office, September 2002), v.

[3] The importance of these emerging threats and DOD's increasing role are addressed in the GAO Report to Congress, *Homeland Defense: DOD Needs to Address the Structure of U. S. Forces for Domestic Military Missions* (United States General Accounting Office, July 2003), 1.

procurement, nor will it address tactical planning in small units and organizations that focus on operating procedures to meet specific tasks. Both of these, while important, bracket the current deliberate operational planning challenge in Homeland Defense, as both military organizational capabilities and tactical competency appear to be sufficient to counter the threat if applied at the right time and place. The current problem is to develop a plan to utilize these strengths in an effective manner against a thinking opponent who seeks surprise and shock- i.e., what to prepare to do at the right time and place.

The military equivalent of this type of contingency planning is the traditional military act of "campaign planning." For military planners, campaign planning is defined as the process whereby combatant commanders and subordinate joint force commanders "translate national or theater strategic and operational concepts through the development of campaign plans" with the resulting campaign plan being a "plan for a series of related military operations aimed at achieving a strategic or operational objective within a given time and space."[4] For plans to protect the Homeland, the "campaign plan" encompasses the emergence of a threat, its detection and characterization, and its eventual defeat. This type of HLS / HLD contingency planning is problematic as organizations struggle to develop plans for both synergistic and synchronized preventative activities required during periods of known but ambiguous threat when a broad operational strategy is required to produce plans. This makes "campaign planning" the most rewarding focus for analysis as a major challenge for HLS / HLD planners because it requires developing a synchronized and effective contingency course of action to counter an evolving and diverse threat environment.

As an organizational system, key shaping decisions for the planning process include determining the degree and timing of senior decision-maker involvement. As "time is the most vital factor" in planning, active and early involvement of military

[4] Definitions from Department of Defense, *Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms*, 12 April 2001. (Washington, DC.: US Government Printing Office, 2001), 59-60.

commanders in making shaping decisions are the most vital factors in planning success.[5] This is especially true of the challenges of military planning for Homeland Defense, which place a burden on military leaders to make contingency plans without clear intelligence on threats and clear forecasting on threat options. To succeed, planners must therefore embrace and overcome the environment depicted in the 2001 *Quadrennial Defense Review*, which described a strategic environment where little is known for certain about precisely where and when a threat will strike and "adapting to surprise – adapting quickly and decisively – must therefore be a condition of planning."[6]

This challenge in protecting the Homeland will continue as the Department of Defense (DOD) and the Department of Homeland Security (DHS) adjust planning processes to address and counter threats of asymmetric attacks on the US from both terrorist groups and hostile nation-states. Because of this lack of certainty and fundamental differences in the structure of the contingency addressed, traditional war-planning does not seem to offer a model to copy for Homeland Defense planning. Whereas traditional planning can be used against a predictive enemy such a "rogue states," asymmetric threats offer no such certainty. A new planning approach called "capabilities-based planning" has gotten a lot of attention inside DOD as the solution to planning uncertainty, including the unique challenges of homeland defense planning.

B. DEVELOPING A CAPABILITIES-BASED PLANNING METHODOLOGY

To address the perceived growing complexity in the global security situation for the United States, DOD is advocating "capabilities-based" defense planning to achieve a broad portfolio of military capabilities that will perform robustly in uncertain future environments. As first formalized in the 2001 DOD *Quadrennial Defense Review*, a capabilities-based approach "focuses more on how an adversary might fight rather than

---

[5] "To a conscientious commander, time is the most vital factor in his planning," warned Korean War commander General Matthew Ridgeway, "by proper foresight and correct preliminary action, he knows he can conserve the most precious element he controls, the lives of his men." As General Ridgeway and countless other military commanders have recorded, pre-campaign planning often is a critical component of victory. A current fundamental tenant in military doctrine is that "planning for the employment of military forces is an inherent responsibility of command." Quotes from Department of Defense, *Joint Publication 5-0: Doctrine for Planning Joint Operations*, 13 April 1995. (Washington, DC.: US Government Printing Office, 1995), I-1.

[6] *Quadrennial Defense Review Report* (Government Printing Office, 30 September 2001), iii.

specifically whom the adversary might be or where a war might occur."[7] To accomplish this broad goal, current DOD capabilities-based planning concept focuses on strategic planning and is expressed in the newest Defense Planning Scenarios used to predict future contingencies. Strategic documents at DOD (e.g. *Strategic Planning Guidance*, *Contingency Planning Guidance*, and *National Military Strategy*) have started adopting this concept by focusing planning "on how adversaries will fight in the future rather than on which specific adversaries we may fight."[8] While not formalizing any definition of what the words "capabilities-based planning" mean (much less how to do it), each document addresses capabilities-based planning as a goal and the way of the future as a mechanism to overcome the nebulous nature of the strategic environment.

The genesis for this approach to planning was strategic thinking at the RAND Corporation's National Defense Research Institute. The author of much of the conceptual work behind the current push for capabilities-based planning is Paul K. Davis at RAND. Davis defines capabilities-based planning as "planning, under uncertainty, to provide capabilities suitable for a wide range of modern-day challenges and circumstances, while working within an economic framework."[9] Though focused on DOD force structure planning rather than campaign planning, Davis believes this new approach to Defense planning is not antithetical to threat-based planning, nor does it solely signify a shift in emphasis from threat to capabilities. Rather, it satisfies the need for increasing variability in Defense planning cases and in the key planning factors for friendly and enemy forces, to better account for uncertainty. For this approach, the question "who is the threat" is addressed as a reworded question "what could the threat *DO*" to allow exploration of a much broader range of eventualities.[10] This helps planners define capabilities needed rather than individual numerical solutions to narrowly defined, highly scripted individual

---

[7] Department of Defense, *Quadrennial Defense Review Report* (Government Printing Office, 30 September 2001), iv.

[8] National Military Strategy 2004 (13 May, 2004), 13.

[9] Paul K. Davis, Analytic Architecture for Capabilities-Based Planning, Mission Systems Analysis, and Transformation (RAND Corporation Publication MR 1513, 2002), 1.

[10] According to DOD Defense Planning Scenario development, "Capabilities-Based Planning is a method of Defense planning that examines a wide range of variability in factors, in order to achieve a broad portfolio of military capabilities that will perform robustly in an uncertain future environment." This unclassified quote is from a classified DOD briefing dated July 2003 from the Office of the Secretary of Defense that accompanied the staffing of the Defense Planning Scenarios.

cases because capabilities-based planning treats the threat as a continuum, within prescribed limits, rather than as a set of single-point values.

A working definition of "Capabilities-Based Planning" modifies these initial DOD and RAND characterizations in order to specifically address the requirements of Homeland Defense and Homeland Security contingency planning for a flexible process that resembles a conceptual "menu" approach to planning. A capabilities-based planning process can therefore be defined as an analytical process of assessing means, capacity, and likelihood of all potentially hostile actors to strike with an emphasis on recasting intelligence uncertainty into a modular "menu" of potential threat capabilities. This planning process would result in a solution framework emphasizing "building blocks" of capabilities that could be tailored to meet persistent general threats or a specific emerging threat.[11] By bracketing potential hostile capacities with assumptions of likelihood facilitates narrowing planning into manageable (and often affordable and acceptable) realms, amorphous threats can be defined and codified to enable planners to develop a list of required capabilities and required authorities and policies to counter anticipated enemy actions while being inherently flexible to changes in the strategic threat environment. Thereby, each new piece of new intelligence further refines what threat capabilities exist and any "actionable intelligence" would trigger the execution of pre-planned defense and security capabilities already identified and enabled.

I intend to use a concept development approach to clarify the definition of "capabilities-based planning" and propose a concept of how to develop a capabilities-based plan for Homeland Defense and Homeland Security missions that will overcome the inherent planning challenges of ambiguous threats and expansive contingencies. In the first chapter, I will first model threat assessment and contingency planning as a Decision Support System to identify required inputs, desired outputs, and critical success criteria for a contingency planning process. The second chapter will apply metrics of an effective planning method to two planning processes, the traditional "threat-based"

[11] This "building block" approach is addressed as a key element in capabilities-based planning in Paul K. Davis, *Analytic Architecture for Capabilities-Based Planning, Mission Systems Analysis, and Transformation* (RAND Corporation Publication MR 1513, 2002), 4.

approach of military planners and the "scenario-based" method currently in vogue with security planners, to demonstrate shortfalls of these two approaches and the need for a new planning process.

The third chapter will begin by examining the history of capabilities-based planning to try to best define what the term means. Then, a "capabilities-based" or "how" approach to threat assessment will demonstrate an effective method to focus on how the threat could attack or act, more than on who are the threat actors. Then, this chapter will describe a process to perform "capabilities-based" planning and demonstrate how this approach can effectively solve current challenges in planning for Homeland Defense and Homeland Security. This capabilities-based planning process will discuss how to identify forces, tasks, and enablers required to counter any likely potential threat capability. Additionally, this chapter will demonstrate how a capabilities-based plan facilitates risk versus resources decision-making by senior leaders by presenting a comprehensive and comprehendible format of threat and friendly capability linkages. The fourth chapter will include two case studies to demonstrate how a capabilities-based plan could be developed by a military HLD command and a civilian HLS organization to reveal practical inputs and outputs of this approach.

Finally, I will conclude with recommendations based on an assessment of the strengths and weaknesses of capabilities-based planning when applied to HLD and HLS operational planning. These recommendations are:

- DOD should halt the use of a traditional threat-based planning process for Homeland Defense contingency planning
- Both DOD and DHS should adopt a capabilities-based approach for threat assessments for Homeland Defense and Homeland Security planning
- Both DOD and DHS should adopt a capabilities-based methodology for Homeland Defense and Homeland Security contingency planning
- Both DOD and DHS should leverage a capabilities-based methodology to formalize linkages between planning and resourcing for Homeland Defense and Homeland Security contingency planning

- Both DOD and DHS should leverage a capabilities-based methodology to formalize linkages between planning and exercises for Homeland Defense and Homeland Security contingency planning

- Both DOD and DHS should leverage a capabilities-based methodology to increase senior decision-maker involvement in Homeland Defense and Homeland Security contingency planning

The goal for this paper is an effective, comprehensive, and explainable planning process that overcomes the inherent challenges in contingency planning against asymmetric threats. A capabilities-based planning process will be defined as an analytical process of templating means, capacity, and likelihood of all potentially hostile actors with an emphasis on recasting intelligence uncertainty into a modular "menu" of potential threat capabilities in order to develop preventative response packages based on means. This conceptual approach has the advantage of being applicable to amorphous threats, flexible for evolving threats, and adaptable for diverse threats. This innovative planning process will demonstrate a solution framework emphasizing "building blocks" of capabilities that could be tailored to meet persistent general threats or a specific emerging threat. Thereby, each new piece of new intelligence further refines what threat capabilities exist and any "actionable intelligence" would trigger the execution of pre-planned defense and security capabilities already identified and enabled. A capabilities-based approach to planning will emerge that will be very effective for Homeland Defense and Homeland Security planning in today's strategic environment because it has the advantage of being applicable for amorphous threats, flexible to evolving missions, effective in facilitating risk versus resources decision-making, and adaptable for diverse agencies.

II. CURRENT CHALLENGES IN HOMELAND DEFENSE AND HOMELAND SECURITY PLANNING

This chapter will identify significant and unique challenges of Homeland Defense and Homeland Security planning. Contingency planning will be developed (and modeled) on the Information Technology concept of a "Decision Support System." Looking at military contingency planning as a Decision Support System (DSS) will isolate required input and desired output to assess various planning approaches as a process. From this assessment, unique planning challenges emerge that establish measures of effectiveness for any Homeland Defense or Homeland Security planning system. This chapter will then assess the advantages and challenges of "threat-based" and "scenario-based" planning methods to show that neither "threat-based" nor "scenario-based" planning effectively addresses the current homeland defense and homeland security planning challenges.

The complex and amorphous post-9/11 threat environment created by the terrorist threat and the unprecedented nature of overlapping Federal, state, and local responsibilities and jurisdictions create unique challenges when planning military and non-military security operations inside the United States. Traditional planning processes appear poorly structured to meet these challenges of HLD and HLS contingency planning because of the diverse and amorphous threat and the need for multiple options for execution that prevent any ability to forecast potential moves and counter-moves. Unlike regional military planning against hostile nation-states, the challenge of assessing asymmetric threats prevents the development of "most likely" and "most dangerous" courses of action. Additionally, only the broadest guidance to thwart the enemy's plans of attack is given to planners due to the absence of detailed analysis of opponents' decision-making systems and a clear understanding of threat tactical and operational goals.

The problem with these traditional approaches is the inability to produce a single course of action option to the decision-makers that can accomplish the broad and diverse preventive missions while countering the diverse threat capabilities available to various hostile actors. With multiple inputs, traditional planning conceptually breaks down because of its inability to present viable courses of action for the commander to assess and select and is poorly structured to provide any certainty on resources required and

risks assumed. Additionally, because the current threat is not solely contingency-based like a war in Korea but rather a steady state of terrorist threat, HLD and HLS planning needs to be constantly cyclic and remove the clear traditional distinction between planning and execution. Because intelligence on the threat is constantly changing and potential methods of attack are consistently evolving, any HLD or HLD plan must be inherently flexible and conceptually be similar to a rheostat approach to readiness wherein preventative measure can be adjusted based on the latest intelligence assessment.

A. WHAT AN EFFECTIVE PLANNING PROCESS WOULD LOOK LIKE

Looking at military contingency planning as a Decision Support System (DSS) isolates required input and desired output to assess planning approaches as a process. This is not a new or unique approach to assessing the planning process as the military has become enamored with Information Technology and Information Management.[12] To assist military commander's with decision-making and the management of on-going events, many versions of military DSS have been developed recently, though the majority are based on using computer displays to track and manage information required for situational awareness and rapid decision-making.[13] But by focusing on the planning process rather than possible uses of emerging information technologies, the requirements and challenges of HLD and HLS contingency planning can be viewed as a DSS in order to determine how these process problems can be overcome. From this assessment, capabilities-based planning emerges as an effective DSS for HLD and HLS contingency planning because it provides decision-makers a "menu" of options to counter the spectrum of threat courses of action. In contrast with traditional campaign planning,

---

[12] This usage of a corporate concept like DSS by military thinkers is not new. Because of fundamental similarities in senior-level executive activities between corporate America and the military, it is only natural that military commanders would look toward cutting edge information management strategies to facilitate executive decision-making that is inherently non-programmed, novel, consequential, and non-repetitive. This paper uses the definition of "executive decision making" from Hugh J. Watson, George Houdeshel, and Rex Kelly Rainer, Jr. Building Executive Information Systems and other Decision Support Applications (Hoboken, N.J.: John Wiley & Sons, 1997), 47-48.

[13] An example of this is the *Commander's Advisory System for Airspace Protection (CASAP)* DSS prototype developed for the 1 Canadian Air Division/Canadian NORAD Region Air Operations Center. This program manages and displays information and provides a series of tools to the military decision-makers to assess proposed courses of action. See Micheline Belanger and Adel Guitouni. *A Decision Support System for COA Selection*. Defense Research Establishment Valcarier, World Wide Web, http://www.dodccrp.org/2000ICCRTS/cd/papers/Track5/049.pdf.

capabilities-based planning also offers a more flexible and dynamic process that can frame required capabilities and overcome uncertainty concerning the threat.

When looking at this planning process, military planning may be considered a DSS, but just what is a DSS? This question needs to be answered up front due to the lack of a shared definition of what constitutes a DSS. Even some recent Information Technology text books admit that there is no real consensus on what characteristics and capabilities constitute a DSS given the varied IT tools labeled as DSS and the wide divergence of tasks for which they are used.[14] While some common references like Introduction to Information Technology base their definition of DSS on a "computer-based information system" approach, others take a more expansive approach.[15] For this paper, DSS will be defined more broadly as "an interactive system that provides the user with easy access to decision models and data in order to support semi-structured and unstructured decision-making tasks."[16] The key here is the focus on decision-making and the executive decision-maker's needs rather than focusing on the information systems and computer systems that are tools in this process.

Applying the definition and concept of a DSS to DOD contingency planning, the military planning process emerges as a DSS that focuses on providing information, analysis, and recommendations to senior decision-makers to assist in the vision and expression of potential courses of action to meet future crises.[17] To further match the DSS concept with the requirements of Homeland Defense planning, contingency

[14] Richard E. Potter, R. Kelly Rainer, Jr., and Efraim Turban. Introduction to Information Technology (Hoboken, N.J.: John Wiley & Sons, 2003), 363.

[15] Richard E. Potter, R. Kelly Rainer, Jr., and Efraim Turban. Introduction to Information Technology (Hoboken, N.J.: John Wiley & Sons, 2003), Glossary G-5. Decision Support Systems and the study of decision-making as a DSS has been around for almost 40 years, beginning in 1965 with computer based model-oriented DSS and currently composing the Web-based DSS of today. Much of the DSS development has focused on information management, business systems, and corporate information systems. But as interactive information systems became common in business, the US Armed Forces began to adapt and adopt DSS and Knowledge Management to facilitate military decision-making. D. J. Powers, *A Brief History of Decision Support Systems*. DSSResources.com, World Wide Web, http://dssresources.com/history/dsshistory.html, version 2.8, May 31, 2003, 1.

[16] This paper uses the definition of DSS from Hugh J. Watson, George Houdeshel, and Rex Kelly Rainer, Jr. Building Executive Information Systems and other Decision Support Applications (Hoboken, N.J.: John Wiley & Sons, 1997), 263.

[17] For the planning process, the focus is on a "strategic model" of DSS that helps senior decision-makers determine the objectives of the organization and the best way to use resources to achieve those objectives. Hugh J. Watson, George Houdeshel, and Rex Kelly Rainer, Jr. Building Executive Information Systems and other Decision Support Applications (Hoboken, N.J.: John Wiley & Sons, 1997), 275.

planning will not address long-range budgeting and organizational planning such as military force structure and procurement, nor will it address tactical planning in small units that focus on operating procedures to meet battlefield tasks. Both of these, while important, bracket the current deliberate operational planning challenge in Homeland Defense as both military organizational capabilities and tactical prowess appear to be sufficient to counter the threat if applied at the right time and place. The problem is to develop a plan to utilize these strengths in an effective manner against a thinking opponent who seeks surprise and shock.

The effective military equivalent of this type of "strategic model" DSS is the traditional military act of "campaign planning." For military planners, campaign planning is defined as the process whereby combatant commanders and subordinate joint force commanders "translate national or theater strategic and operational concepts through the development of campaign plans" with the resulting campaign plan being a "plan for a series of related military operations aimed at achieving a strategic or operational objective within a given time and space."[18] This is the most rewarding focus for DSS analysis as "campaign planning" is a major challenge for Homeland Defense planners. It requires developing a synchronized and effective contingency course of action to counter an evolving and diverse threat environment.

While there are many forms of effective campaign plans or contingency plans, each was the result of an efficient planning approach with many shared characteristics. Metrics of a good plan and effective planning methodology include a process that is flexible to evolving threats and emerging information on the threat. The process must be adaptable to different organizations, especially the lower level tactical and operational agencies that will execute the resulting plan. Measures of an effective plan also include being comprehensive to all operations and contingencies the plan is designed to address. The overall objective of contingency planning is to overcome operational uncertainty with flexibility in planning to produce living documents with options and branches that are fundamentally different from many contingency plans produced using traditional

[18] Definitions from Department of Defense, *Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms*, 12 April 2001. (Washington, DC.: US Government Printing Office, 2001), 59-60.

planning processes. Many of these plans appear to be detailed rigid plans that fill volumes on the shelf but offer as the only decision for senior leaders is to approve the execution, sit back, and watch. The measure of a good plan is the flexibility of options to produce plans that are the antithesis of the Schliffen Plan of 1905, where the government of Germany was presented only the option to invade both France and Belgium in response to Russian mobilization because their plan was based on rigid mobilization and movement timelines.

Additionally, because the objective of any planning process is to facilitate senior level decision-making on resource allocation and risk assessments, both the process and the resulting plan must be understandable by senior decision-makers. This ensures both senior leader involvement and the ability to make sound choices. By leveraging senior leader involvement, a clearly comprehensible planning process should also clearly identify risks and recommendations on mitigation strategies to increase chances of success. The result of this planning process also must provide a linkage between the plan and required resources to identify decision points to decision-makers. The last requirement of an effective plan is a linkage between the plan and the organization's exercise and training program to provide the mechanism to validate and modify the plan.

B. PROBLEMS WITH CURRENT PLANNING METHODOLOGIES

The *National Security Strategy* identifies the vital function of having a formal and deliberate process of assessing threats, yet a viable and effective process to do this has yet to gain wide acceptance. When military planners use the words "threat assessment," they are not just referring to any information or intelligence about potential opponents or enemies. They are also referring to the formal process of how this intelligence is analyzed and portrayed. Considering that the level, scope, and specificity of the intelligence to be assessed is often beyond the control of the planners, which approach or process is taken in the analysis phase is all the more critical in shaping the intelligence product sought: a "threat assessment." Conceptually, there are three different fundamental approaches to conducting a threat assessment, with a focus on either the "who," the "what," or the "how" of the threat. In a traditional threat assessment, the process addresses the "who" of the threat – who is the threat actor, what is their "order of battle" and what are their most

likely courses of actions. The second conceptual approach to threat assessment is to look at the "what" of the threat – what part of the threat is a specific agency's responsibility to defeat and what aspect of the threat must the planner address typically in a limited number of "threat scenarios."

However, both "threat-based" and "scenario-based" planning will not work effectively for Homeland Defense or Homeland Security planning because the asymmetric threat cannot be templated and is both uncertain and adaptive.[19] Advocates of capabilities-based planning assert that it is this strong potential for the threat to achieve surprise by asymmetric means that makes threat-based and scenario-based planning a poor match for the needs of emerging planning challenges like Homeland Defense and Homeland Security. This is because:[20]

- Threat-based planning is very susceptible to threat deception, causing the US to mischaracterize and often underestimate the threat
- Planners traditionally tend to "mirror image" threats when little hard intelligence is available which is only effective for symmetric threats
- Large bureaucracies like DOD tend toward group think and discourage "out of the box" thinking required to understand and assess asymmetric threats
- Resource constraints tend to focus time and money on traditional big ticket weapons systems and discourage development of capabilities for the "unproven" asymmetric threats

As this list reveals, the reasons behind recent examples of the US being surprised by asymmetric enemies in a manner not addressed in existing contingency plans are all linked to the threat-based planning culture that laid deep roots during the Cold War. The memories of 9/11 and the fears of unprecedented terrorist capabilities combine with these

[19] In expressing the variety of threats facing the US, the current *National Strategy for Homeland Security* (NSHLS) states, "Homeland security is focused on terrorism in the United States…Terrorists can be U.S. citizens or foreigners, acting in concert with others, on their own, or on behalf of a hostile state." Statements like this define three main types of threats facing America today: a continuation of conventional military threats from hostile nation-states, traditional asymmetric threats from hostile states and state-sponsored political groups, and a new trans-national terrorist threat from ideological enemies. The US Homeland is confronted with a spectrum of threats ranging from traditional national security threats (for example, ballistic missile attack) to law enforcement threats (for example, drug smuggling) and countering these threats requires a series of formal threat assessments. *National Strategy for Homeland Security* (Government Printing Office, July 2002), 2.

[20] These four challenges for threat-based planning is detailed in the chapter "Responding to Asymmetric Threats" in *New Challenges, New Tools for Defense Decisionmaking* edited by Stuart Johnson, Martin Libicki, and Gregory F. Treverton (RAND Corporation Publication MR-1576-RC, 2003), 43-44.

uncertainties to drive Homeland Defense and Homeland Security planners to search for a planning process that avoids these pitfalls.

1. Failure of a Threat-Based Planning Approach

While utilizing the most modern information technologies, the current DOD planning process is based on traditional thinking and organizational habits adopted during the Cold War.[21] Military contingency plans during the Cold War – a powerful historical foundation for the current generation of planners and senior leaders – were perceived by most as symmetric confrontations with a known enemy, which created cultural expectations of force-on-force combat and an acceptance of "mirroring" capabilities and intent in planning.[22] This traditional military approach to planning is a threat-based approach that focused single contingency plans on a single enemy or combination of enemies – a conceptual "who" approach to the threat based on known hard data and assessment of leadership and decision-making. The goal of this process was a single course of action recommended to national strategic decision-makers that was portrayed as a series of moves and counter-moves proposed to thwart an enemy whose capabilities and intents had been forecasted in detail from decades of assessment.[23] Even after the demise

---

[21] Because of the formal and bureaucratic nature of current DOD planning, the complex Joint Operation Planning and Execution System (JOPES) process is codified in a series of published memorandums from the Chairman of the Joint Chiefs of Staff (CJCS). The first CJCS memorandum on JOPES, called Department of Defense CJCSM 3122.01, *Joint Operation Planning and Execution System (JOPES), Volume 1 (Planning Policies and Procedures)*, lays out the policies and procedures for all of DOD to follow. This thick manual of approximately 400 pages is followed by three additional volumes of CJCS JOPES memorandums that provide details as to formats and procedures for planners. In addition to supporting instructions, labeled as CJCSI, this series of thick manuals is the intellectual foundation for modern military contingency planning. Department of Defense, CJCSM 3122.01, *Joint Operation Planning and Execution System (JOPES), Volume 1 (Planning Policies and Procedures)*, 14 July 2001. (Washington, DC.: US Government Printing Office, 2001), enclosure C, C-3.

[22] This practice resulted in plans having tables and tables of numbers and specifications of military hardware like ballistic missiles, tanks, planes, ships comparing US / Allies and Soviet / Warsaw Pact equivalents. Paul K. Davis, *Analytic Architecture for Capabilities-Based Planning, Mission Systems Analysis, and Transformation* (RAND Corporation Publication MR 1513, 2002), 34-35.

[23] As a result of growing concerns with strategic "flashpoints" and the necessity of detailed planning to move the forces and logistics of the US military, producing and updating campaign plans became one of the key roles of military commanders. As a recent theorist on military information transformation proposed, "given the limits of Industrial Age communications, *plans* were the mechanisms by which military commanders sought to create the conditions necessary for success." Because of this, "large, complex organizations in particular depended on comprehensive plans that required considerable time to prepare and also had to be continuously monitored, adjusted, and maintained." David S. Alberts, and Richard E. Hayes. Power to the Edge: Command…Control… in the Information Age (Washington, DC.: Command and Control Research Program, CCRP Publications, 2003), 47.

of the focus on the expected clash in central Europe, this threat-based approach seemed effective in the post-Cold War world for nation-state opponents such as North Korea and Iraq.

For senior military decision makers, the key point in the process is the concept development phase that is focused on mission analysis, threat assessment, and course of action development. Mission analysis is a formal tool for planners to determine the specific mission essential tasks that must be performed in order to successfully achieve the assigned objectives. When combined with the determined purpose for the plan, mission analysis produces the mission statement for the plan, the shaping of which is a key step for the military commander to express his vision for the contingency plan. Next, a formal Threat Assessment is produced from national intelligence estimates and information. For planners, an Intelligence Estimate is the "appraisal, expressed in writing or orally, of available intelligence relating to a specific situation or condition with a view to determining the courses of action open to the enemy or potential enemy and the order of probability of their adoption."[24] The threat assessment is usually portrayed as "most likely course of action" and "most dangerous course of action." This leads to an anticipated single line of action for the threat, most often depicted as a chronological series of actions.

From these assessments of mission and opposition to that mission, planners then develop options for the commander which are most often in the form of proposed courses of action (COAs). For military planners, a COA is defined as "a possible plan open to an individual or commander that would accomplish, or is related to the accomplishment of the mission," often expressed in terms of concept of operations (or execution concept), risk assessment, resources requirements, and resource shortfalls.[25] While various staff elements (operations, logistics, legal, communications, etc.) determine supportability and feasibility of the proposed COAs in "Staff Estimates," it is the development of the options for the commander and the selection of the "Commander's Concept" or

[24] Definition from Department of Defense, *Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms*, 12 April 2001. (Washington, DC.: US Government Printing Office, 2001), 209.

[25] Definition from Department of Defense, *Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms*, 12 April 2001. (Washington, DC.: US Government Printing Office, 2001), 130.

recommended COA that most shape the early output of traditional military planning. The decisive point in Concept Development is the presentation to the senior decision-maker of options on courses of action that accomplish the assigned mission and address likely and dangerous options available to the enemy.

An outline of the DSS process for concept development can be expressed as a simplified version of the traditional military planning process showing required input and desired outputs (see Figure 1).[26] The inputs that feed this system are strategic guidance that aims to spell out the goals and parameters for the forecasted contingency and intelligence products that the intelligence community provides in as much detail as possible on obstacles and enemies who oppose the achievement of those goals. The staff then produces a mission analysis and an intelligence estimate by assessing and synthesizing this information. Approving this foundation for concept development is the first of two major involvements by the military commander in his role as senior decision-maker. The first set of decisions by the commander shapes the rest of planning by focusing efforts on specific mission essential tasks, often expressed in the commander's chosen verbiage, and on expressing what the enemy is expected to do, could possibly do, and is capable of doing. By having the commander approve the threat estimate, planners are able to view and plan against the threat as the senior decision-maker sees it. The last input to concept development is the commander's formal chance to issue "Initial Planning Guidance," often expressed by the commander's desired endstate, method for achieving success in the mission, and how the commander sees the operation or planned campaign supporting larger national strategic efforts.

---

26 The deliberate military planning process is a five phase system that starts the flow of planning from the first phase of plan initiation where strategic guidance and threat intelligence shapes the tasks assigned to the plan. From this guidance, planners develop a strategic concept during Phase II through a structured process of concept development and produce a proposed course of action to be reviewed and approved during the third phase. After a course of action has been approved by senior decision-makers in DOD, Phase III involved detailed planning required to develop and coordinate the forces, logistics, and transportation required to execute the plan. When this detailed plan development is complete, Phase IV involved review and approval of this detailed plan, leading to the last phase wherein all supporting and subordinate commands developed their own supporting plans for the approved course of action. As this reveals, what each phase does is tied to the evolution of the course of action proposed in Phase II and to the involvement of the senior decision-makers in shaping the final plan. Department of Defense, CJCSM 3122.01, *Joint Operation Planning and Execution System (JOPES), Volume 1 (Planning Policies and Procedures)*, 14 July 2001. (Washington, DC.: US Government Printing Office, 2001), enclosure C, C-9.

With these foundational pieces in place, and in language shaped by the senior decision-maker himself, the planners are ready to develop varied options and courses of action for achieving the commander's desired endstate. As the planners narrow planning on a handful of courses of action, the staff works to wargame the COAs to determine feasibility and desirability, resulting in the next intervention of the military commander. This takes place in the often-formal "Course of Action Decision Brief" whereby the commander selects his concept for how the operation will unfold. Once the commander selects a course of action and issues additional guidance for planning, the last step of Concept Development occurs as the staff fleshes out the concept with additional details. The result is an approved Strategic Concept, often described as the "base plan," that is then expanded in plan development into a detailed document which can be hundreds of pages long for major regional warplans. As this description reveals, the current JOPES planning process can be expressed as "an interactive system…to support semi-structured and unstructured decision-making tasks" - which makes this system a planning DSS.[27]

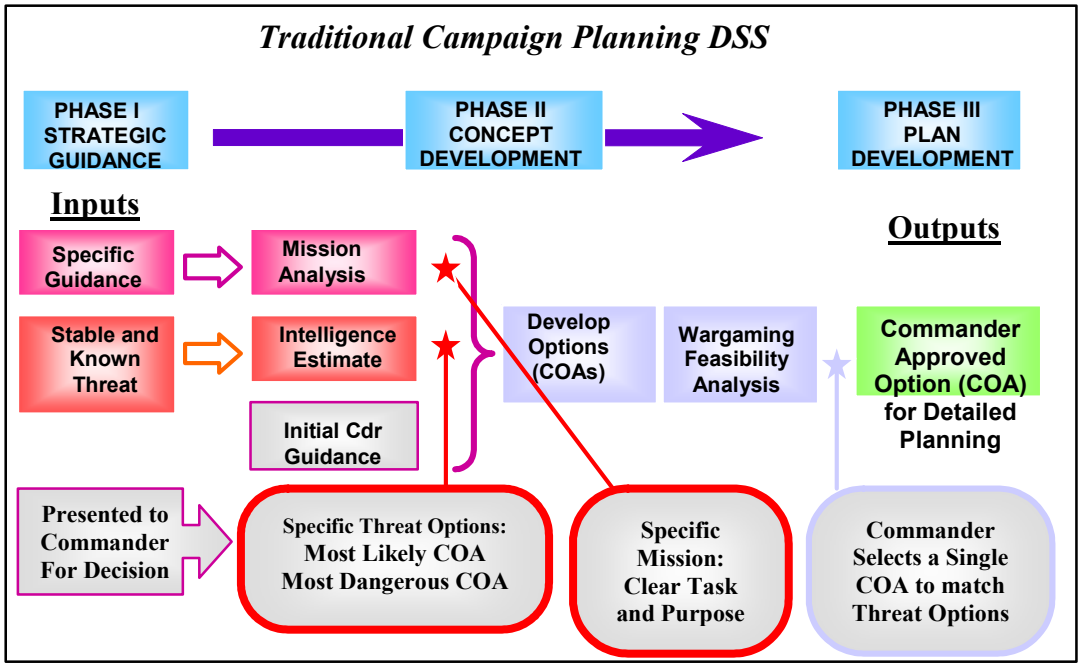

Figure 1. Military Campaign Planning as a Decision Support System.

[27] This paper uses the definition of DSS from Hugh J. Watson, George Houdeshel, and Rex Kelly Rainer, Jr. Building Executive Information Systems and other Decision Support Applications (Hoboken, N.J.: John Wiley & Sons, 1997), 263.

The clearest example of the strength and dominance of this traditional DOD approach to the planning process was recent war planning for the invasion of Iraq. When seeking to understand what could happen and reactions to US moves, both military planners and analysts in the intelligence community relied on traditional threat information such as equipment in armored divisions, location of artillery units, ranges of missiles, historical profiles of key leaders, all forms of measurable data. From these knowns, analysts developed an Iraqi "order of battle" based on a traditional organization chart. When combined with knowledge of the Iraqi leadership's formal decision-making process, this "who" approach also produced a relatively detailed menu of anticipated courses of action, based on the large volume of information known of the Iraqi government and Iraqi military. Planners then developed and refined the plan through a conceptual series of action-reaction cycles to predict what operations were required to achieve the desired end-state. For this nation-state opponent, planners believed the threat-based assessment provided a solid foundation to plan the Coalition campaign. The result was a smashing success against the Iraqi leadership and especially against the conventional Iraqi military. While the planning for the Coalition campaign to depose Sadaam Hussain was in many ways innovative and unique, the process of plan development and senior leadership review that was used was very traditional and at times bureaucratic.

This recent experience reinforced the idea that traditional campaign planning is best thought of as a DSS to reveal how the key phase for senior leader involvement is concept development because this is where commanders shape the campaign and make decisions on threats and options. One of the critical products for decision-makers in concept development is the "intelligence estimate" or "threat assessment." As current DOD doctrine asserts, "intelligence should provide the commander with an understanding of the adversary in terms of the adversary's probable intent, objectives, strengths, weaknesses, probable COAs, most dangerous COA, values, and critical vulnerabilities."[28] Based on this threat assessment and strategic guidance, planners will develop a single course of action with branches and sequels. This traditional planning

[28] The importance of this military function is the common theme of current military doctrine on intelligence. See Department of Defense, *Joint Publication 2-0: Doctrine for Intelligence Support to Joint Operations*, 09 March 2000. (Washington, DC.: US Government Printing Office, 2000), I-4.

process results in decision-makers selecting a single contingency plan with a "throw the switch" type decision being the result. Therefore, traditional military planning process is a DSS with a single decision chain. This was possible during the relatively stable strategic environment of the Cold War when even complex plans for major theater wars could go years with only slight modifications.[29]

Planner acceptance and understanding of an innovative approach to planning like capabilities-based is made all the more difficult by the pervasiveness of the threat-based process cemented during the Cold War. However, this threat-based planning approach requires a level of detailed intelligence that is just not available for today's trans-national terrorist threat. Post-war planning in Iraq revealed the bottom limit for intelligence hard data required for the traditional planning process. Even knowing the shortfalls of this traditional approach, most emerging threats to the Coalition forces were originally expressed as supporting conventional military forces. During the drive on Baghdad, intelligence analysts (and TV pundits) searched asymmetric and terrorist groups like the "Saddam Fadayeen" and "Mohammed's Army" for formal plans, organizational structures, and chains of command as if they were made up of conventional hierarchical units. Only after the first chaotic months of Coalition occupation was this approach modified, reflecting a recognition that insufficient information was available on an asymmetric enemy whose non-hierarchical cell structure offered few targets for conventional military operations. Anticipating problems like this, one planning analyst concluded, "planning that is threat based requires an established threat. When adversaries hide the details of their threats, it can take years or even decades (if ever) to uncover," placing the US at a disadvantage and almost ensuring surprise will be achieved by asymmetric threats.[30]

---

[29] "Thus, even though hierarchies are relatively slow [to adapt], they could keep pace with a fairly stable security environment, which characterized most of the 20th Century." David S. Alberts, and Richard E. Hayes. Power to the Edge: Command…Control… in the Information Age (Washington, DC.: Command and Control Research Program, CCRP Publications, 2003), 225.

[30] Paul K. Davis, Analytic Architecture for Capabilities-Based Planning, Mission Systems Analysis, and Transformation (RAND Corporation Publication MR 1513, 2002), 46.

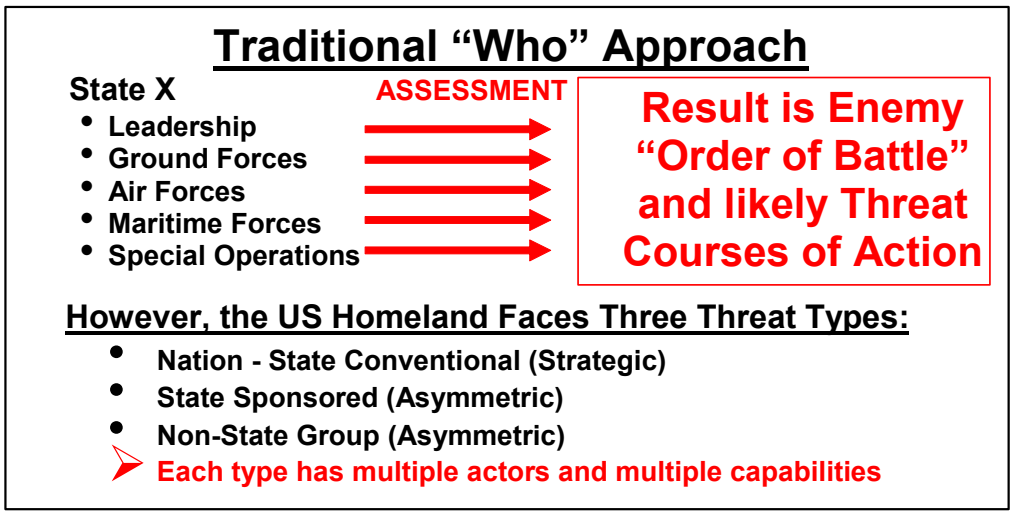

Figure 2. Traditional Approach to Threat Assessment.

Even after the demise of the focus on the expected clash in central Europe, this threat-based approach seemed effective in the post-Cold War world for nation-state opponents such as North Korea and Iraq (see Figure 2). However conceptually simple this traditional "who" approach is for a threat like the North Korean military, when looking at the complex combination of state, state-sponsored, and non-state threat actors that the US Homeland faces, this threat-based planning process produces only guesses and vague pictures of potential threat actions. This is because of the lack of hard intelligence of al Quida's organizational structure, operational capabilities, and strategic plan of action required to develop a viable action-reaction conceptual framework. Without knowing how many "cells" are operating, how they receive operational guidance, and where specifically they plan to strike, planners have little certainty to base plans on. While intelligence successes in the global war or terrorism have been filling in the blanks on many questions, the absence of a template and historical data will continue to frustrate those who seek to apply a traditional "who" approach for the unprecedented threats to the US Homeland. This requirement for factual data and historical templates drives the current search for "actionable intelligence" that will fill in the blanks and reveal projected threat actions and anticipated reactions to potential defensive operations.

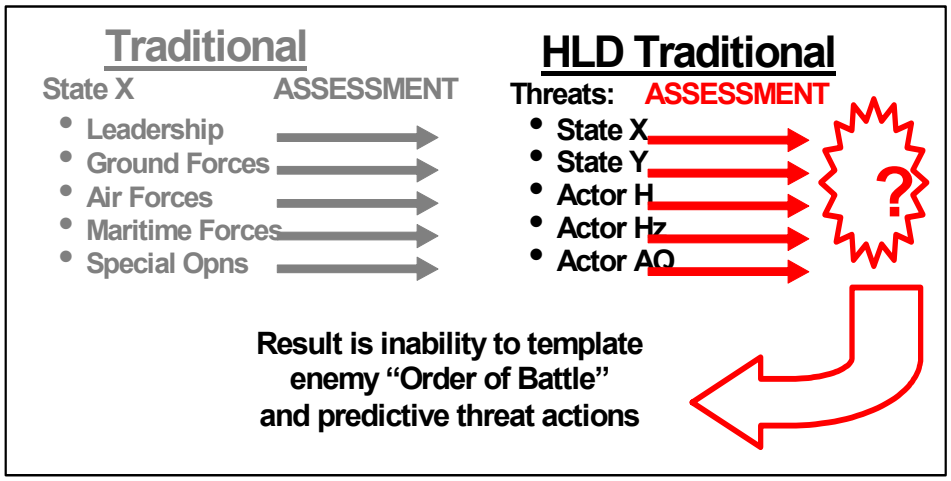

Figure 3. Failure of Traditional Threat Assessment.

Because of the inherent secrecy and covert structure of groups like al Quida, this "actionable intelligence" is in short supply and is unable, even for those who have access to classified detainee debriefs and communications intercepts, to provide a confident assessment of planned and on-going operations. This is not a challenge that will likely be overcome in the future as trans-national terrorist groups are making secrecy and protection of this information a priority through encoding messages, building non-hierarchical cell structures, an ideological and not hierarchical decision-making process, and amorphous relationships between various terrorists groups and supporters. The result will most likely be a continuation of the intelligence situation where very few specifics are known. For all these reasons, taking a traditional threat-based planning approach in an asymmetric and unprecedented threat environment can be inherently frustrating because of the absence of enough hard intelligence and results in continued inability to template a terrorist "order of battle" and determine any form of predicted threat likely courses of action (see Figure 3).

While functional for traditional war planning, the very nature of the current diverse and amorphous threat to the US Homeland prevents any traditional military planning process from producing effective security and defense plans. Unlike regional planning against hostile nation-states, the challenge of assessing the asymmetric Homeland Defense threats prevents the development of "most likely" and "most dangerous" courses of action. Additionally, only the broadest guidance to thwart the enemy's plans of attack is given due to the absence of detailed analysis of opponents'

decision-making systems and a clear understanding of threat operational and strategic goals. For these reasons, the traditional planning DSS appears poorly structured to meet the challenges of Homeland Defense contingency planning because of the diverse and amorphous threat and the need for multiple options for execution that prevent any ability to forecast potential moves and counter-moves (Figure 4).

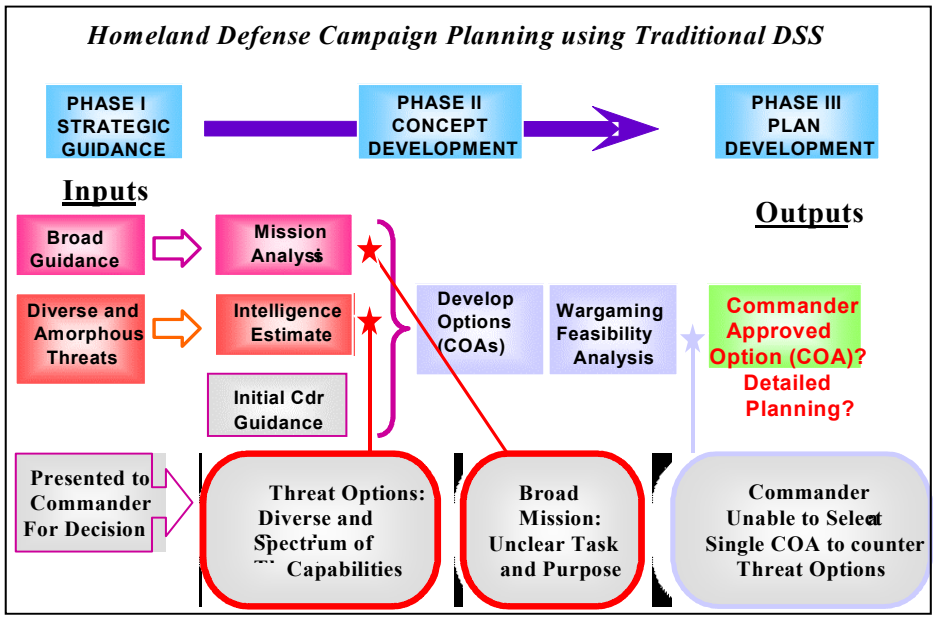

Figure 4. Homeland Defense using a Traditional Campaign Planning Decision Support System

Because of the nature of the inputs into any HLD contingency planning, the mission analysis and intelligence estimate steps cannot accurately template how threat actions will likely unfold, which is a requirement in order to produce a course of action that would counter anticipated contingencies. In other words, the problem with the traditional approach is the inability to produce a single course of action option to the commander that can accomplish the broad and diverse Homeland Defense missions while countering the diverse threat capabilities available to various hostile actors. With multiple inputs, traditional planning conceptually breaks down because of its inability to present viable COAs for the commander to assess and select. Because of these diverse inputs in guidance and threat assessment, the traditional planning process is simply unable to be restructured to deliver multiple outputs – not a single COA, but a "menu" of options to counter the menu of options available to asymmetric threat actors. Therefore, the inherent

challenges in Homeland Defense planning include the inability to template the threat and the inability to develop a single course of action that promises to counter the threat. Effective Homeland Defense (and Homeland Security) planning process must overcome these two problems.

2. Failure of a Scenario-Based Planning Approach

After 9/11, many HLS planners tried a different approach to contingency planning by using a "scenario-based" planning process that focused on what events could happen. This approach was based on "what if" drills that postulated a limited number of threat actions and then wargamed agency responsibilities for potential counters. The process of this scenario-based approach was best seen at the Salt Lake City Olympics where planners from various agencies with counter-terrorism and consequence management responsibilities did "what if" drills and coordinated their planned responses. This use shows the advantages of this method of planning as it is very simple in execution and can be modified based on what scenarios are selected. These "what if" contingency plans also have the benefit of not requiring a detailed threat assessment as issues and questions concerning the threat can be mitigated by making assumptions to fit the scenario. Though conceptually simple, and therefore attractive for initial planning efforts, this approach does have weaknesses because effective "scenario-based" planning requires certainty about possible scenarios and a limited number of scenarios to plan against.

An inherent problem with this "what if" method is unavoidable – scenario-based planning only produces plans for the contingency scenarios selected. For example, all of these challenges were revealed in 2002 when DOD facilitated a Homeland Security and Homeland Defense series of tabletop exercises to wargame existing contingency plans in what became labeled as the "Nine Scenarios." The goal of this planning exercise was to clarify DOD responsibilities during the stand-up of the Department of Homeland Security. However, during the initial meetings, there was little agreement as to what scenarios to utilize because of lack of consensus on the most likely "what ifs" – a return to the need for "actionable intelligence" to discern what, how, and where the terrorists were going to strike next. As a result, nine very broad scenarios such as "attack on a port" and "biological attack" were selected, multiple branches and variations of each scenario were developed. The process was reduced to a discussion of what would be the most

challenging scenarios (a lengthy list of extreme contingencies) and a conscious dismissal of any attempt to determine a limited and manageable number of likely "what if" contingencies. The end result was disagreement on reasonable scenarios and little progress on wargaming and planning due to an inability to get past discussions on the scenarios themselves – what DOD planners are told to avoid, "fighting the scenario."

The Department of Homeland Security (DHS) recently attempted to overcome this challenge by formalizing a set of standard threat scenarios in order to establish an accepted baseline for planning and funding response incidents and crises. This form of "universal threat" planning is designed to be the foundation for the development of all HLS "national preparedness standards from which homeland security capabilities can be measured."[31] Because of the current counter-terrorism focus and concern for potential mass casualty attacks, DHS introduced a formal threat baseline of "threat scenarios" that city planners are to use to evaluate their current level of manning, equipping, and planning for prevention and recovery capacity. While utilizing a scenario-based planning process, even the introduction to these "planning scenarios" stresses the need for capabilities-based planning and emphasizes that "for domestic incident preparedness to proceed through a capabilities-based approach."[32]

However, this effort has also run into resistance from HLS planners because of claims that "one size does *not* fit all." This scenario-based approach makes claims of flexibility with "ways that allow them to be adapted to local conditions," but offers a framework of set tasks and agency roles that cannot be easily modified.[33] City planners and decision-makers are quick to point out that each city is in fact unique with some having mass transit, some having port facilities, and all having different venues for large gatherings and different levels of threat from overseas terrorists. This standardized approach also intrinsically offers no flexibility to modify the scenarios for local or changing conditions. The challenge for any scenario-based approach is being able to plan

[31] Homeland Security Council, Planning Scenarios: Created for Use in National, Federal, State, and Local Homeland Security Preparedness Activities, July 2004 (Washington, DC., 2004), iii.

[32] Homeland Security Council, Planning Scenarios: Created for Use in National, Federal, State, and Local Homeland Security Preparedness Activities, July 2004 (Washington, DC., 2004), vi.

[33] Homeland Security Council, Planning Scenarios: Created for Use in National, Federal, State, and Local Homeland Security Preparedness Activities, July 2004 (Washington, DC., 2004), iii.

with certainty that the scenarios developed will be "the" scenarios that will be faced. That certainty is a rare and perishable commodity in the diverse planning community that addresses the multifaceted and ambiguous threats to the US Homeland.

Secretary of Defense Donald Rumsfeld expressed a simple idea when he pointed out, "Our [DOD] job is to close off as many of those avenues of attack as possible. We must prepare for new forms of terrorism, to be sure, but also for attacks on U.S. space assets, cyber-attacks on our information networks, cruise missiles, ballistic missiles, and nuclear, chemical, and biological weapons."[34] This requires a different approach from developing a "Universal Task List" of a limited number of generic scenarios that all agencies and locals are to plan for. "Closing off" the ability of threat actors to use methods of attack – i.e., their "capabilities" – is the goal of capabilities-based planning. The process of capabilities-based planning outlined in this paper is a flexible approach that can be both adapted and adopted. A scenario-based planning process inherently limits the flexibility of the planners. In focusing on what a threat can do rather than threat scenarios, the flexibility inherent in capabilities-based planning: allows any organization at any level to build a menu of their own capabilities or develop a menu within a menu of what is required to support the larger counter-terrorism efforts. In contrast to the inflexible nature of a "Universal Task List," capabilities-based planning enables rapid revision of plans to address changing strategy, threats, capabilities, or political / military dynamics and provides up-to-date options for senior decision-makers of any organization.

Because the first step of any effective contingency planning process is to assess the diverse and complex threats to the Homeland in a manageable and coherent process, these "who" and "what" approaches to Homeland Security and Homeland Defense threat assessment both have difficulty producing the answers required by planners. However, a "how" approach to the threat is more promising because of its applicability to a more nebulous and unstructured threat environment. For this approach, the question "what is the threat" is addressed as a reworded question "what could the threat *DO*." Utilizing all

[34] Donald H. Rumsfeld, "Transforming the Military," *Foreign Affairs* Volume 81, Number 3 (May/June 2002).

the information available, regardless of specificity, analysts using this process seek to define and assess what threat capabilities *any* potential hostile nation-state or non-state group might use.

THIS PAGE INTENTIONALLY LEFT BLANK

III. A CAPABILITIES-BASED APPROACH TO CONTINGENCY PLANNING

Because of diverse inputs in guidance and threat assessment, the traditional planning process is simply unable to be restructured to deliver multiple outputs – not a single course of action for prevention of attacks, but a "menu" of options to counter the menu of options available to asymmetric threat actors. This push for more options forms the basis for the push for a capabilities-based planning process that can meet the requirement of delivering a "menu" plan for complex and amorphous contingencies in Homeland Defense campaign plans at US Northern Command (USNORTHCOM). After the challenges of HLD planning since 9/11, the combatant commander of USNORTHCOM tasked his HLD planners to develop a plan that could link required resources with anticipated risks. Without a clear enemy order of battle, the commander believed any effective preventative plan must identify the specific resource cost and answer the question, "what do these resources buy?" Additionally, any HLD planning process must consider risk and address the question, "where and how much is an acceptable level of risk for this Plan?" Because of these factors, a traditional approach to planning that is threat-based appeared ill prepared for such an amorphous and dynamic planning environment where so little is known about the enemy's plans and arsenal while the threats' intentions to do harm are crystal clear.

This chapter will show that by using a capabilities-based approach to threat assessment, the question "who is the threat" is reworded as "what could the threat *DO*" to allow exploration of a much broader range of eventualities and give HLD or HLS planners a defined and detailed threat to plan against. When military planners use the words "threat assessment," they are not just referring to the information or intelligence about potential opponents or enemies, but also about the formal process of how this intelligence is analyzed and portrayed. Considering that the level, scope, and specificity of the intelligence to be assessed is often beyond the control of the planners, which approach or process is taken in the analysis phase is all the more critical in shaping the intelligence products sought: a "threat assessment." Though each of these conceptual approaches to threat assessment is valid for some types of planning, this chapter will

demonstrate that a "capabilities-based" approach to threat assessment has the advantage of being applicable to amorphous threats, flexible for evolving threats, and adaptable for diverse threats.

This chapter will then focus on demonstrating a method to conduct capabilities-based planning that will overcome the planning challenges identified in the last chapter. The capabilities-based planning process will identify forces, tasks, and enablers to counter any likely potential threat capability. While conceptually straightforward, this approach to planning against threat capabilities requires the same level of work and wargaming in order to develop effective contingency plans, but what is different is the ability to simply both *understand* and *express* what is being done about specific threat scenarios and calculate, explain what resources are required, and identify specific resources devoted toward countering each threat capability.

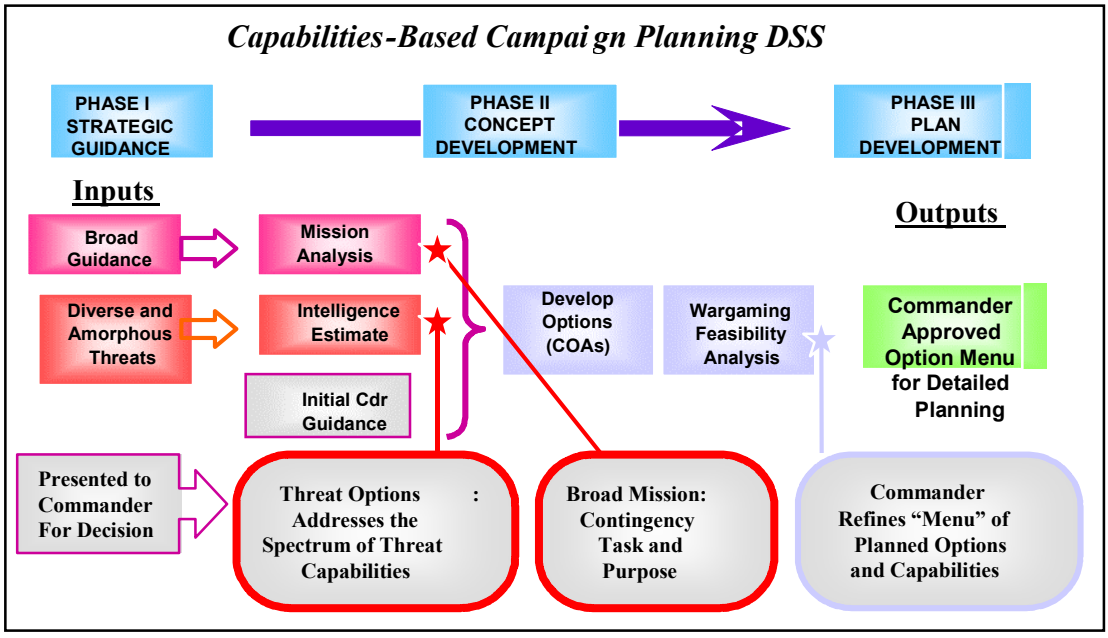

Figure 5. Capabilities-Based Planning Decision Support System.

This push for more options forms the basis for the push for a capabilities-based planning process that can meet the requirement of delivering a "menu" plan for complex and amorphous contingencies in Homeland Defense campaign plans. The requirement is for a flexible process that resembles a conceptual "menu" approach to planning. A capabilities-based planning process can therefore be defined as an analytical process of

assessing means, capacity, and likelihood of all potentially hostile actors to strike with an emphasis on recasting intelligence uncertainty into a modular "menu" of potential threat capabilities. Therefore, capabilities-based planning provides senior military decision-makers with a DSS that has the inherent flexibility to address Homeland Defense contingency planning (Figure 5). This required planning process would result in a solution framework emphasizing "building blocks" of capabilities that could be tailored to meet persistent general threats or a specific emerging threat.[35]

This menu approach of capabilities-based planning provides more flexibility for Homeland Defense planning. The challenge for Homeland Defense decision-makers is the need to adopt a DSS that can adapt to a changing and dangerous environment. This is not just an issue of new communications and computer technologies, but must emphasize and facilitate the critical role of strategic and operational decision-making. While discussing the growing complexity in organizational decision-making, a recent Management Information article on DSS supports this conclusion by asserting, "organizations and their decision support systems must embrace procedures that can deal with this complexity and go beyond the technical orientation of previous DSS."[36] Often, the decisive point of whether a key decision will be made in an effective and timely manner is not on the computer screen, but between the ears of the decision-maker. "To assure these advanced information technologies provide maximum benefit to the user, the Army needs to incorporate …adaptive decision-aiding capabilities," concludes one military researcher, "these technologies will achieve their optimal effectiveness only if they are compatible with the cognitive capabilities and limitations of the commanders, staff and soldiers who will use them."[37] This challenge starts at the selection of a process to assess the threat.

---

[35] This "building block" approach is addressed as a key element in capabilities-based planning in Paul K. Davis, *Analytic Architecture for Capabilities-Based Planning, Mission Systems Analysis, and Transformation* (RAND Corporation Publication MR 1513, 2002), 4.

[36] James F. Courtney, *Decision Making and Knowledge Management in Inquiring Organizations: Toward a new Decision-Making Paradigm for DSS.* ScienceDirect: Decision Support Systems, World Wide Web, http://www.sciencedirect.com/science.html. Decision Support Systems, Volume 31, Issue 1, May 2001, 17.

[37] Thomas H. Killion, "Decision Making and the Levels of War," in *Military Review*, US Army Command and General Staff College, November – December 2000, 70

A. DEVELOPING A CAPABILITIES-BASED THREAT ASSESSMENT

A new conceptual approach needs to be found to structure and assess threats in Homeland Defense contingency planning. A solution to this challenge can be found in the concepts of "lines of operation" and "capabilities" as dynamics to define and explain potential and likely threat-friendly interaction. As oppose the spatial or temporal divisions of the battlespace by borders, domains like air and seas, and phasing like build-up, defense, and offense, Homeland Defense campaigns are shaped by a reactive concept to threat actions and the division of the threat into potential lines of operation. "Lines of operation" are defined by the Department of Defense as "lines that define the directional orientation of the force in time and space in relation to the enemy."[38] For Homeland Defense and Homeland Security operations, these lines of operation can be modified to address distinct and related methods of both attack and defense such as "maritime attacks" or "attacks on continuity of government."

These lines of operation for the threat can then be defined and depicted in terms of specific capabilities. The Department of Defense dictionary defines a "capability" as "the ability to execute a specific course of action (a capability may or may not be accompanied by an intention)."[39] Having a capability implies the ability to perform a set of tasks required to accomplish the mission requiring the capability. This intentionally very broad definition covers both capabilities involved in strategic organizational issues like force sizing and procurement and operational issues like tactics and weapon performance. For this paper, a capability is defined as the ability to perform the task set out in the capability within the conditions and performance standards accepted for that mission set. Therefore, the capability to conduct a "swarm boat attack" includes the ability to plan and execute multiple simultaneous attacks on maritime targets using small boats with an expectation of causing significant damage to the targets. However, it is important to highlight that this does not imply that the group with this capability has the plan or the intent to use this specific capability in their next attack.

---

[38] U.S. Department of Defense. *Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms*, 12 April 2001 (Washington, DC.: US Government Printing Office, 2001), 246.

[39] U.S. Department of Defense. *Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms*, 12 April 2001 (Washington, DC.: US Government Printing Office, 2001), 60.

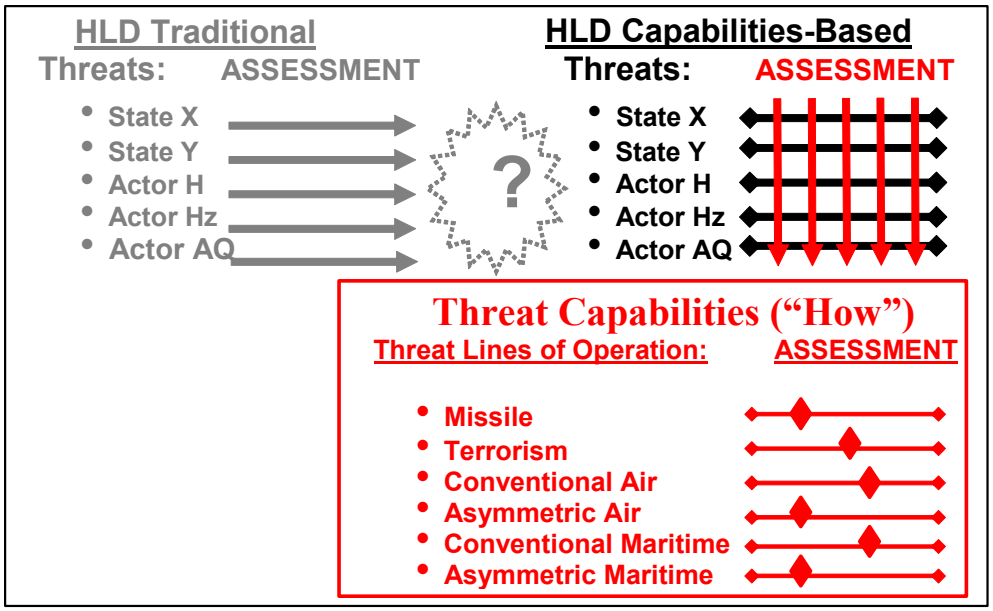

Figure 6. A Capabilities-Based Approach to Threat Assessment.

In addressing the question "what is the threat," this "how" approach aims to produce a matrix of possible (and likely) threat capabilities that need to be countered by assessing the threat by capability and not by group or actor (see Figure 6). For example, with a potential of multiple actors possessing the means and the will to conduct terrorism in the US Homeland, the focus of assessment is not al Quida, but any potential terrorist group; what terrorist acts (or capabilities) are possible? Now the question becomes manageable within current information limits because the intelligence analysts are no longer predicting what or where al Quida will strike next, but how could any terrorist could strike. In this manner, a capabilities-based threat assessment is done by first assessing what types of threat lines of operation are possible to bring threat capabilities against the US (i.e., – Ballistic missiles? Terrorism? Air attack?). Then for each type of threat faced, threat lines of operation or "red lines" of threat capabilities can be developed to identify specific methods to deliver threat capabilities. Even this rudimentary level of analysis can assist planners in providing a framework for the threat environment. The combination of "lines of operations" and "capabilities" inherent in capabilities-based planning allows an intellectual structure to address the many challenges in HLD planning.

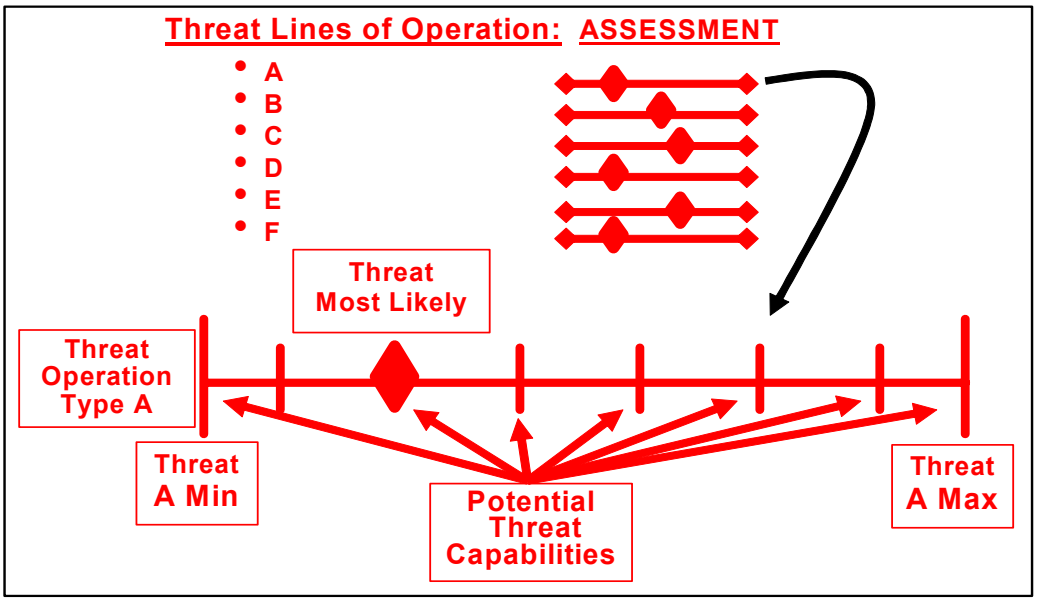

Figure 7. Developing Threat Lines of Operation and Threat Capabilities.

The same assessment can then be done for each threat type to identify possible hostile capabilities. In building these threat lines of operation or "red lines," intelligence can be used, not to dictate what exactly trans-national terrorist groups and rogue states are most likely to do, but rather to determine the range of possibilities – the maximum and minimum threat each group posses to the US Homeland (see Figure 7). For example, the threat of ballistic missiles is both complex (due to the technical nature of the method) and well-understood (due to the limited number of threat actors and the physics involved). However, what exactly is the threat? If the threat of strategic attack is developed as a threat capability type, a relatively simple example of a threat line of operation emerges. Even though missile defense rests on hard data of numbers and ranges, developing a maximum and minimum limit to this threat "red line" helps frame the answer to the threat question and helps missile defense planners by scoping the challenge (and defining the required HLD capability). For example, the minimum threat to the US Homeland is not zero – the potential for accidental launch or North Korean strategic miscalculation ensures that; and the maximum is not the combined strategic arsenals of Russia, China, France, Great Britain, Israel, India, Pakistan, and North Korea. In this manner, following through this intellectual process of analysis also helps both analysts and planners by graphically representing an intellectual framework for the threat environment.

While intelligence information may reveal glimpses of the ideology and goals of various threat actors, the simple formula of "threat ideology plus capabilities equals likely targets and courses of action" cannot be used a tool for threat assessment because ideology is rarely easy to assess and often can lead to simple – and incorrect – predictions of threat actions. Problems with an ideological approach can surface on two levels during the threat assessment. First, a single group's ideology, often the group judged to be the most dangerous, can be superimposed on all threats, artificially narrowing potential threat courses of action and possibly overlooking equally likely capabilities. For example, the perceived aim of al Quida is often offered as the goals of "fundamental Islamists," but the numerous diverse groups under this label have disparate and often contradictory ideological objectives. Additionally, there is the complex and difficult problem of accurately determining a threat groups ideology from the outside, based on partial and limited information. For these reasons, the key for a viable assessment framework is to broadly focus across potential threats and not focus on the perceived ideology of a single threat actor. The proposed capabilities-based approach allows for this by integrating known threat information on ideology and likely activities by limiting the spectrum of templeted capabilities within a framework of a maximum and minimum threat framework addressed on each "red line."

The terrorist threat to US ports and maritime commerce can be developed as an example of a "capabilities-based" threat line of operation. The first step is an assessment of all potential threat actors and methods of attack within the parameters of a "red line" based on the method of threat operation and their target rather then simply the borders of the domain (i.e., – a cruise missile attack on a port can be considered a "maritime attack" even though it is an air-breathing flying weapon). By looking at all potential threat capabilities, analysts evaluate threats from both state and non-state actors and consider any likely method of attack and sort each capability by magnitude of impact.

By building a spectrum of specific and distinct threat capabilities along a single line of operation, analysis of current intelligence on each threat actor can help define what constitutes "likely" threats that are feasible and anticipated means of attack and can shape the minimum and maximum of the threat along the developing threat "red line" (see Figure 6). Intelligence can also guide the designation of a "most likely" attack

method for each group and a collective "most likely" capability (seen in the red diamond on the threat "red line") for the entire threat line of operation. The result is a coherent and comprehensive threat assessment for a threat such as the notional "transnational air attack" line of operation depicted in Figure 9.

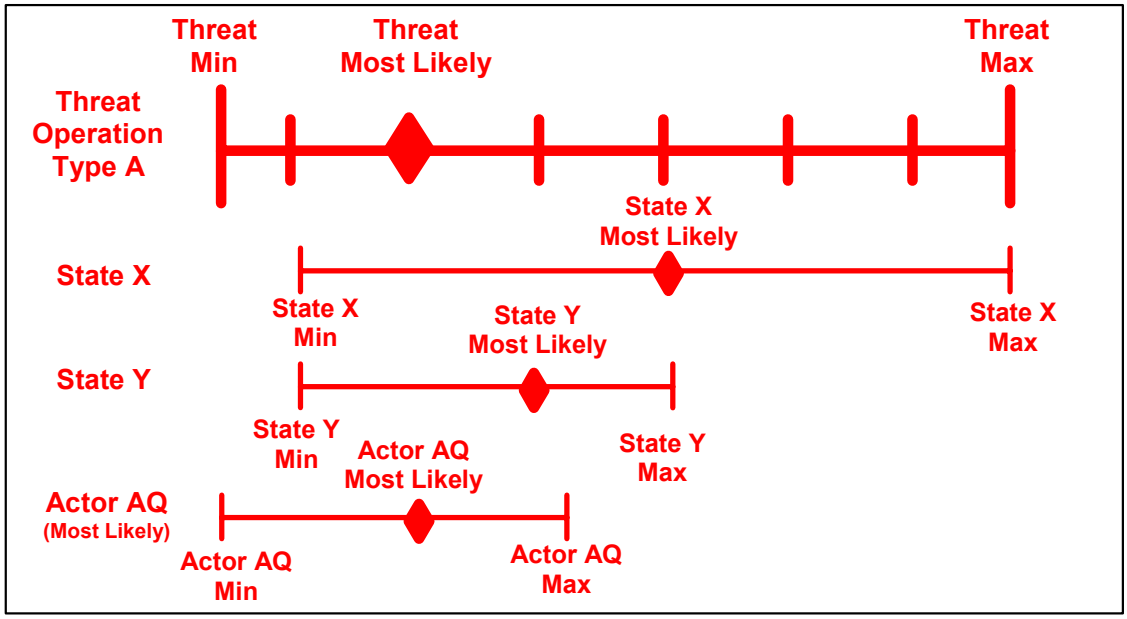

Figure 8. Developing an Assessment of Threat Capabilities.

Bracketing potential hostile capacities with assumptions of likelihood facilitates narrowing planning into manageable (and often affordable and acceptable) realms. Between these two assumed limits are then templated other possible threat capabilities associated with this threat type regardless of which threat actor processes this capability or method of attack. In this manner, amorphous threats can be defined and codified to enable planners to develop a list of required capabilities and required authorities and policies to counter anticipated enemy actions while being inherently flexible to changes in the strategic threat environment. In essence, this enables an amorphous threat to be assessed as a menu of distinct (and conceptually simple) attack "capability" types with assigned degrees of likelihood and magnitude. Each new piece of intelligence then further refines what threat capabilities need to be depicted and any "actionable intelligence" would trigger the execution of pre-planned defense and security lines of operation already identified and enabled.

This "how" process also has the advantage of being conceptually simple, though complex and detailed in practice and open to constant conceptual refinement. An example of a simplified (and notional) capabilities-based threat assessment can be seen in the transnational air attack threat line of operation in Figure 8. This line of operation for the threat would be built to include all unconventional asymmetric air threats aimed at the US Homeland, but tailored for the responsibility and role of the organization conducting the assessment. In this way, while each numbered capability point is subject to challenge and dissection, the holistic nature of the threat and what needs to be countered are graphically represented. Then current intelligence on various threat actors would determine the most likely threat threshold as seen by the red diamond depicted at capability G7. For the "transnational air attack" line of operation (if conducted with actual intelligence available), the product from this process would answer questions on the threat while being flexible to changing conditions on threat actors, intent, and capabilities.

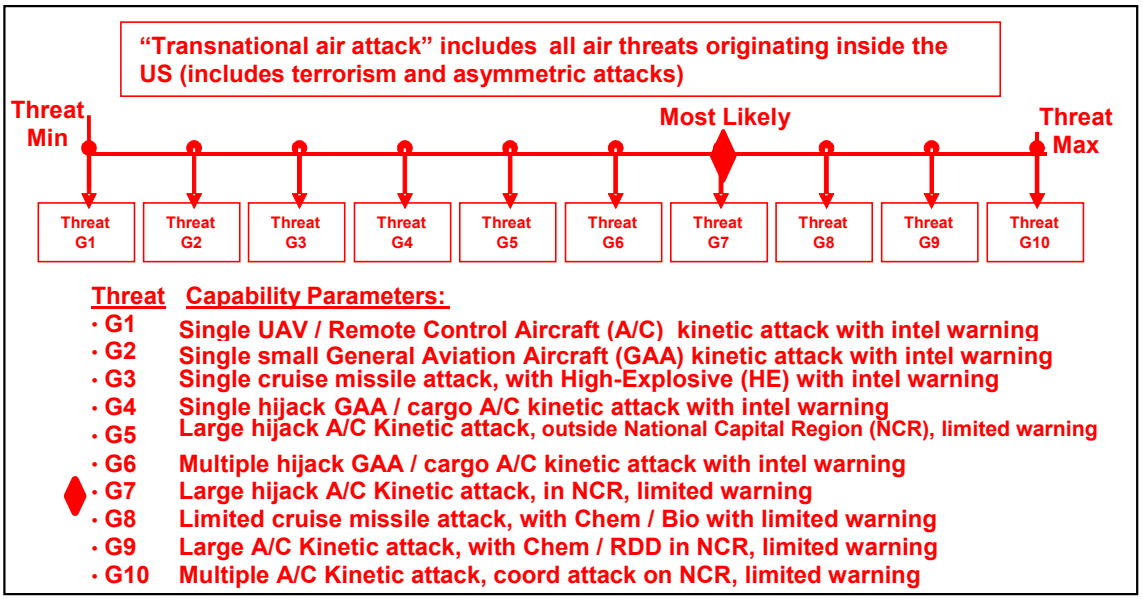

Figure 9. Example of Capabilities-Based Threat Assessments (Illustrative Purpose Only).

This capabilities-based approach to threat assessment can also work for HLS-type threats where agency responsibilities overlap. An example of a simplified (and notional) capabilities-based HLS threat assessment can be seen in the transnational threat line of operation involving land attacks as depicted in Figure 9. In this example, eight threat capabilities are determined to be the potential "how" the enemy might attack and the three lowest magnitude capabilities (H1, H2, H3) are determined to be the most likely. This threshold "red diamond" of assessed probability can be adjusted by intelligence "chatter" or perceived changes in vulnerabilities (for example, during a special event). While focusing planners on the most likely threat, this capabilities-based assessment also depicts other, less-likely threats (H4 – H8) that must be addressed in contingency planning due to their greater magnitude and potential impact. While greatly oversimplified, these example "red lines" show enough assessment of the threat that planners can identify and develop defensive lines of operation and capabilities needed to counter these threats.

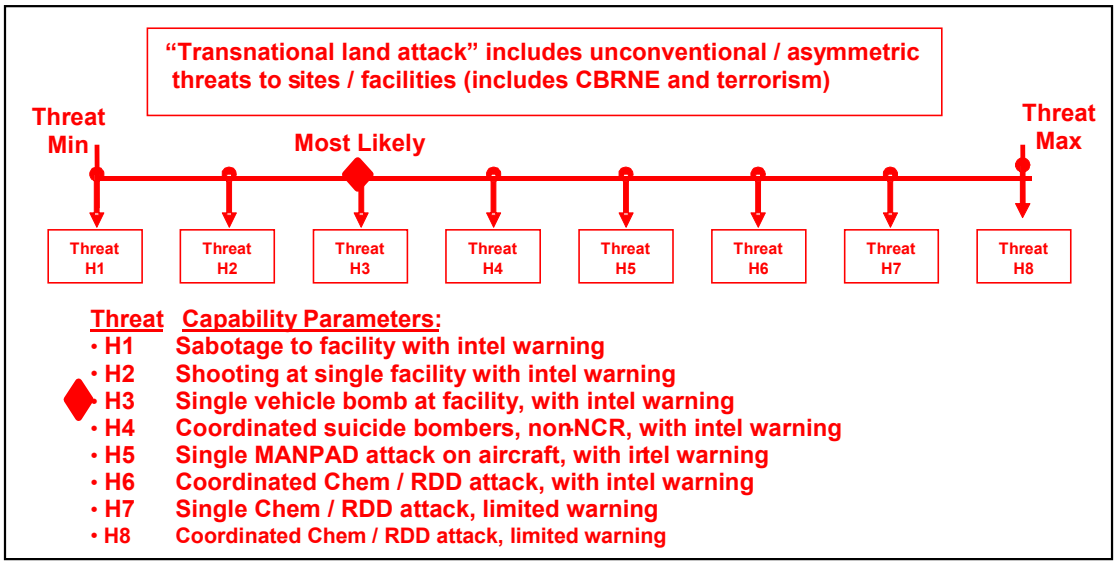

Figure 10. Example of Capabilities-Based Threat Assessments (Illustrative Purpose Only).

While this "how" assessment is a distinct process from traditional approaches to threat assessment, this focus on threat capabilities integrates the strengths of threat-based ("who") and responsibilities-based ("what") approaches. From threat-based, all available hard data on the threat can be integrated into an assessment of likely capabilities,

maximum and minimum threats. This threat-based data is also required to define what each capability entails and its capacities and limitations (for example, defining what constitutes a "Vehicle Borne Improvised Explosive Device" or "VBIED" and what are possible delivery means). Additionally, assessments of current intelligence indicators and hostile leadership communications can focus efforts on certain threat lines and certain threat capabilities. As a result, the knowledge of the threat from a "threat-based" approach can be integrated into the proposed approach in the development of likelihood of the use of threat capacities and in determining the limits of these threat capabilities.

At the same time, each threat capability addressed on a threat line of operation ("red line") can be seen as an individual scenario that can be wargamed within a larger framework. Integrating the value of this type of "what" approach, each threat capability (i.e., capability point on a threat "red line") can be exercised as a possible scenario for planners and senior leaders to wargame agency responsibilities and required authorities. Also, certain "red lines" and threat capabilities could be identified as being a different agency's responsibility, but these assumptions have now been formalized and a mechanism identified to validate these divisions of responsibility. In this way, capabilities-based threat assessment is a viable and synergistic process of answering the simple and fundamental question "what is the threat" by focusing on "how" a threat could attack the US Homeland. Furthermore, this process is scalable and the resulting assessments could be as complex, or as simple, as the planning needs dictate.

B. DEVELOPING A CAPABILITIES-BASED MENU OF OPTIONS

The key to the capabilities-based plan is a direct linkage between threat capabilities and required friendly capabilities to counter them. As the threat has been assessed into a set number of capabilities and defined with a minimum and maximum potential threat, the friendly line of operation required to counter the threat can be bounded into a similar set of capabilities bounded by the same minimum and maximum as depicted in Figure 10. Then, each threat capability is examined to determine what can be done to negate this capability and prevent its successful execution by treating each as a distinct and individual threat scenario. For each specific threat capability to be successfully executed, certain threat actions must be done in sequence concerning

planning, preparation, transit, and execution, all which can be wargamed even with a limited amount of detailed and unambiguous knowledge about specific threat actors and tactics. From this discrete and defined scenario of potential threat actions, an individual "blue" capability plan can be formed by then basically asking what can be done to stop this action. The parameters of each capability data point can be expressed as planned protective and preemptive measures directed generically against the possible threat attack method.

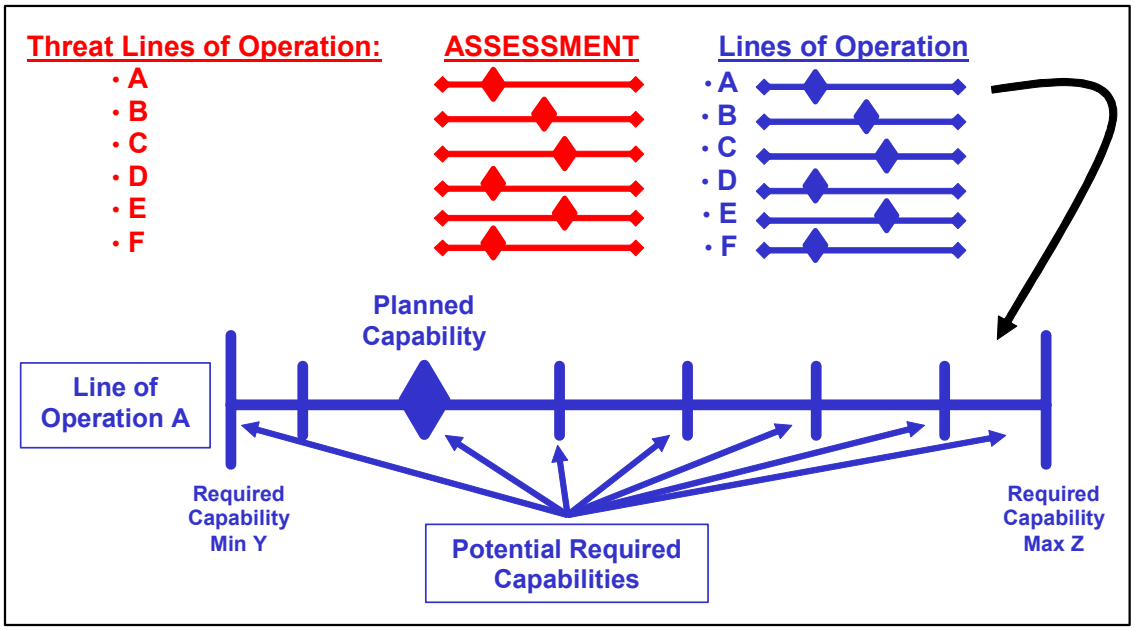

Figure 11. Capabilities-Based Planning Concept.

While intelligence assessment of threat capabilities set the red diamond (likely threat), the experience and judgment of senior decision-makers establish the appropriate blue diamond or "planning threshold." This is not simply a matter of matching the anticipated likelihood of threat attacks because reasoning on vulnerabilities and intent of the organizational leadership may decide to either over-match the threat by placing the blue diamond at a higher magnitude than the red or by accepting a greater risk by lowering the level of resource commitment. Additionally, setting the planning threshold at a certain point does not necessarily negate or ignore all threat capabilities along the higher end of the threat lines of operation because planners can still establish contingency plans for the emergence of a set or all of these less-likely, but higher magnitude threat

capabilities. In this way, the planning threshold or "blue diamond" just differentiates between "Be Prepared To" type tasks with dedicated resources and unresourced contingency tasks without eliminating any likely threats from planner attention and decision-maker consideration.

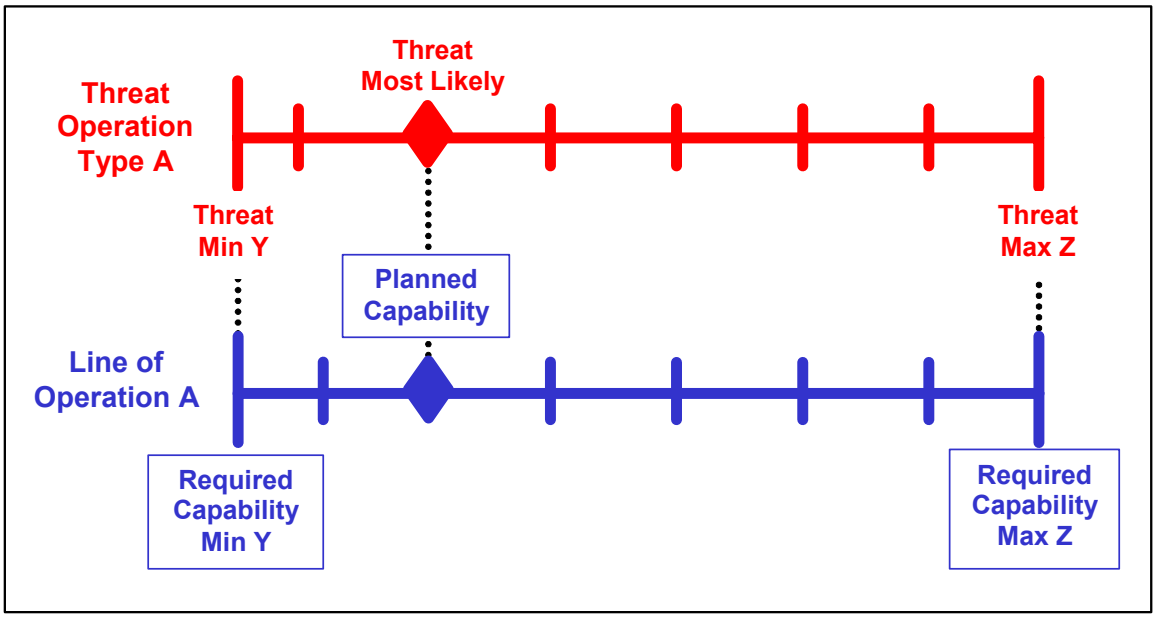

Figure 12. Countering Each Threat line of Operation.

The development of individual lines of operations and specific capabilities can also be a method to integrate diverse capabilities and coordinated multiple organizations into a joint response. Because various capability experts are simply being asked "what can they *DO* to counter a specific threat capability," detection, preventative, and defensive activities can all be integrated into a single capability package and expressed as a single capability data point along the appropriate friendly line of operation (i.e., collected at a single point along a "blue line"). This matrixed planning can be as detailed as required and each capability point can be "drilled down" in order to establish a coordinated and synchronized preventative package. However, the strength of this approach also is that each capability point can be simplified and expressed to senior leadership for the difficult decisions on resources and risk.

Additionally, the same straightforward question can be asked of different agencies and organizations in order to build a coordinated (and commonly understood) response to counter a specific threat capability. Planners from subordinate or outside organizations

can develop independent preventative lines of operation with unique and redundant capabilities assigned to counter the assessed threat capabilities (red lines with data points). Following any guidance on assignment of tasks and overall mission(s), leadership intent, and end state objectives, planners can then produce their own organization's assessment of required capabilities (blue lines with data points) and resources required at each blue data point. After each agency has developed potential counter capabilities, these capabilities can be integrated (and redundancies removed) by simply combining the lines of operation and incorporating the designated capabilities at each planned capability.

An example of this approach could be seen in how a "blue line" could be developed against the notional "transnational maritime threat" line of operation. Because each of the labeled capability data points along the threat line of operation is a specific maritime threat scenario, HLD and HLS planners can address each in turn to determine what their own organization could do to counter that individual asymmetric maritime threat aimed at the US Homeland. For example, to counter the most-likely threat capability, planners would assess all possible preventative actions within their assigned responsibilities and geographic area that could be used to defeat an attack of a single boat-bomb with limited warning due to the ship with the bomb not being previously identified as a "vessel of interest." The resulting matrix of specific actions would include detection measures such as harbor patrol, prevention measures such as waterside obstacles and buoys, and defensive measures such as armed guards on board selected vessels and a more heavily armed quick response force. The resources required for this capability would then become known, as would warning time required to generate non-standing capabilities and the requirement for standing detection mechanisms to provide that warning time. While this example is grossly oversimplified, planners could use this approach to whatever level of detail required and then wargame each red capability against the proposed response to determine any shortfalls.

This example also demonstrates the inherent flexibility and adaptability of this approach to planning because the discover or suspicion of a new threat capability or the emergence of a new threat group with an innovative line of operation against the US Homeland would dictate the addition of blue points or possibly even entire new blue lines

of operation. But this could be done during wargaming or even during crisis action planning without disrupting the larger concept of operation and planning approach. Decision-makers could also remove red lines and threat capabilities as threats are degraded or responsibilities shift between organizations. Resetting the "planning threshold" for each defensive line of operation can also be adjusted based on the latest threat intelligence queuing and decision-makers' judgment of the environment. This inherent flexibility and cyclic nature of capabilities-based planning helps integrate contingency planning and current operations by removing the distinction between how the two are expressed and assessed.

Because each friendly capability is matrixed individually, the process of determining resource requirements is both relatively simple and dynamic in a changing environment. The resources needed for each individual capability along each line of operation can be added and, after removing possible resource duplication, the total cost in personnel, equipment, and funding can be easily calculated. Because each capability data point can be considered as its own scenario and can be made as detailed as required with specific parameters and shaping assumptions, the resource requirements for each can be determined by asking the simple question, "what types and what amounts of resources does your organization need to counter this specific threat?" For senior decision-makers and operators alike, this establishes a key linkage between resources and assessed threats in straightforward manner.

Additionally, this process will reveal required "enablers" such as staff support tasks, standing or pre-designated command and control relationships, pre-approved authorities for using force, concept of employment for any alert forces, and coordinated surveillance tasks required for the planned capabilities (blue lines) to be executed. This can be done through internally wargaming the prevention plan at each capability point to determine what non-resource requirements -in communications, coordination, and authorities for example – were shortfalls or roadblocks to successful execution. This type of structured, but flexible mini-scenario assessment and discussion can also facilitate coordination of which organization can most effectively deliver enablers and capabilities for prevention. By combining required resources with needed enablers, the cost of each

"menu" item can be easily determined and clearly expressed as building blocks in capability to facilitate senior decision-makers assessment of where the planner threshold should be established.

C. A CAPABILITIES-BASED APPROACH TO RISK VERSUS RESOURCES DECISION-MAKING

While this planning process allows for the identification of resources required at each point on blue lines of operation to deliver the needed capabilities, setting the planning thresholds allows senior decision-makers to have a deliberate mechanism to allocate resources and assess risks. This capabilities-based planning method addresses the concerns of the current USNORTHCOM combatant commander by calculating and expressing the answers to the two key decisions "what do these resources buy?" and "where and how much is an acceptable level of risk for this Plan?" As seen in Figure 11, the process of matching threat capabilities and counter capabilities intentionally facilitates this decision-making judgment on resources versus risks by expressing the "building blocks" of capabilities as requiring a set amount of resources to mitigate the risk of the threat capability they are built to counter. When the planned (and resourced) threshold is placed to match the most likely assessed level of threat, that amount of dedicated resources can be stated as counter that level of risk, as well as less robust threat capabilities (i.e., a preventative capability for multiple truck bomb attacks could be claimed to address the threat of a single truck or car bomb). However, planners may recommend, and decision-makers may select, to either assume a greater degree of risk and move the "Planned Capability" threshold to the left (only address lower magnitude threat capabilities) or increase the resource commitments to "buy down" risks of less-likely, but greater magnitude threat capabilities (see Figure 12).

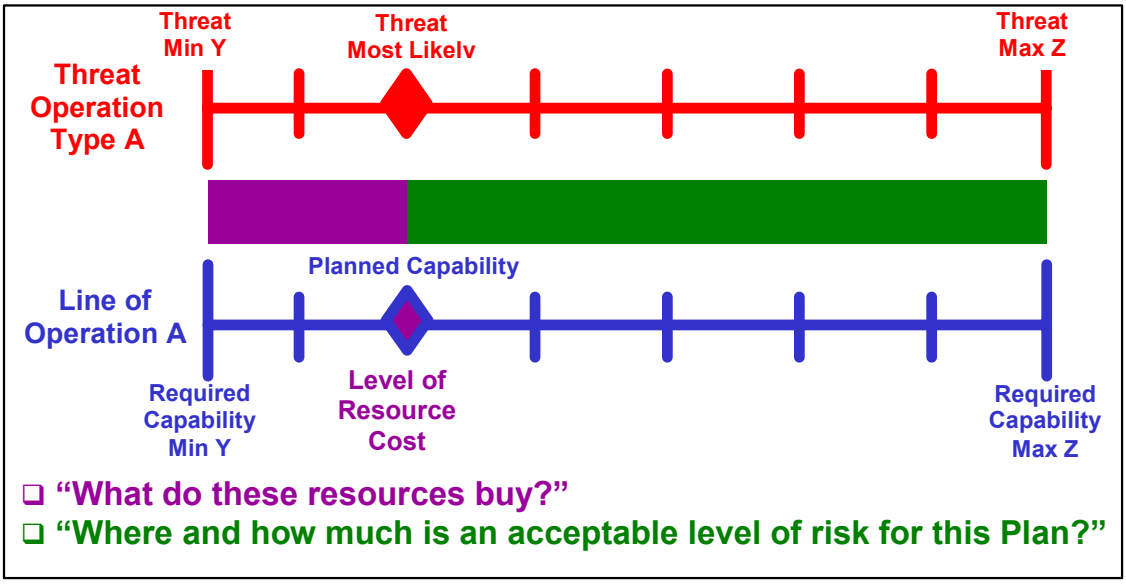

Figure 13. Assessing Resource Levels and Risks.

As seen in the simple graphic above, this planning method addresses one of the major challenges by providing a formal mechanism to simplify complex contingency plans for presentation to senior decision-makers. By overlaying threat lines of operation ("Red Lines") with preventative lines of operation ("Blue Lines"), this can be done without oversimplifying resource and risk decisions or confusing the linkage between assessed threats and planned counters. While the intelligence assessment will determine the most-likely threat level and the placement of the red diamond on a threat line of operation, this approach appropriately places the decision of establishing the planned capability threshold or blue diamond where it belongs – in the hands of senior decision-makers. But unlike more traditional approaches to HLD and HLS planning, now this decision is better facilitated and the risk versus resources trade-offs better understood and expressed.

With reliance on plans expressed as capabilities and on graphically comparing likely threat capabilities and possible methods of attacks with friendly capabilities to counter them, this approach also can be used to identify and mitigate mismatches in capabilities. As depicted in Figure 13, this is conceptually as basic as comparing likely threat capabilities and available prevention capabilities. Where no counter capabilities exist, mitigating long-term risks require investment and research strategies to develop

what is required. Once the red lines and blue lines are compared to determine other shortfalls, mitigation strategies can also be developed on short-term risks. There are three possible ways to address capabilities mismatch: increase preventive capabilities (move "Blue Diamond" to the right), degrade / attack threat capabilities (force "Red Diamond" to the left), or accept risk for threat capabilities (identified as short term shortfalls). The important take away from the analysis portrayed in Figure 13 is that this approach allows for a method of both developing and expressing these mismatches to senior decision-makers.

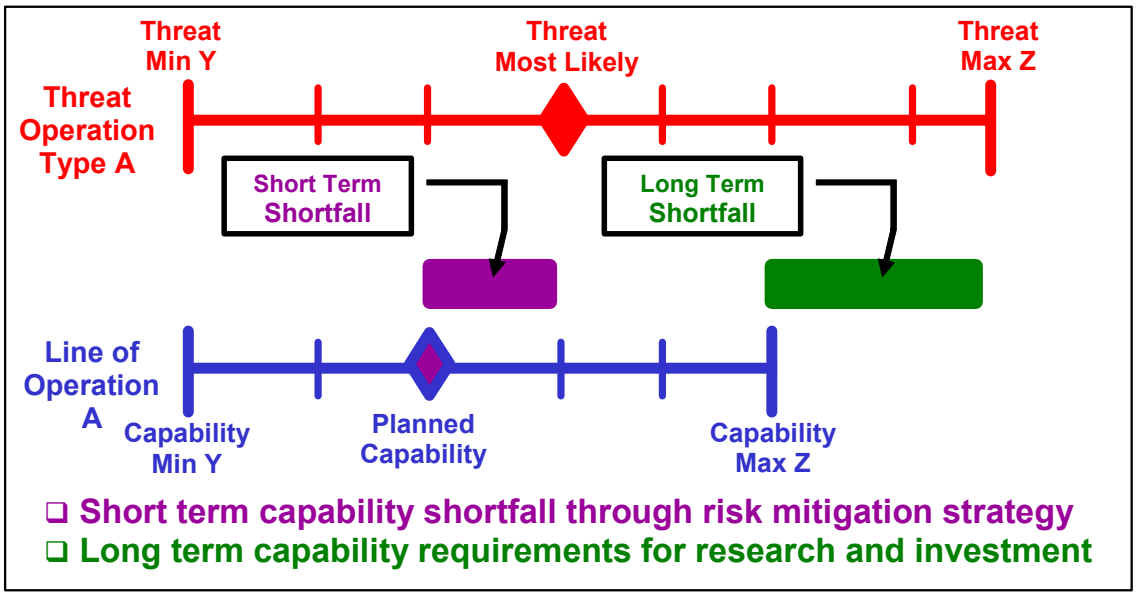

Figure 14. Determining Capabilities-Based Shortfalls.

While these examples are simplified, the entire process is conceptually straightforward and the outcome is a method to develop and present contingency planning to senior decision-makers. Once the capabilities-based plan is complete, the result is a solution framework emphasizing "building blocks" of capabilities that have been planned out, resourced, and wargamed and that could be tailored to meet persistent general threats or a specific emerging threat.[40] This allows the choice of specific or comprehensive responses to threat warnings. If a single threat emerges or threat warning is received concerning a single threat line of operation (such a warnings of a hijacking or warnings of attacks involving aircraft), a single line of operation ("air defense") can be

[40] This "building block" approach is addressed as a key element in capabilities-based planning in Paul K. Davis, *Analytic Architecture for Capabilities-Based Planning, Mission Systems Analysis, and Transformation* (RAND Corporation Publication MR 1513, 2002), 4.

conducted to counter this specific threat. However, if the threat is more comprehensive, such during a war overseas or a period of vulnerability such as a major military deployment of forces, a more wide-ranging posture can be executed to counter all possible threat capabilities.

This capabilities-based approach to planning introduces both flexibility and adaptability by helping planners define a menu of capabilities needed rather than numerous individual solutions to narrowly defined, highly scripted scenarios. Capabilities-based planning treats the threat as a continuum, within prescribed limits, rather than as a set of single-point values. This highlights one weakness in the concept: a more specific intelligence warning is intrinsically required to determine the "where" and the "when" of the threat attack and the detailed tactical planning of where counter capabilities need to be executed. However, often intelligence warning can provide some narrowing information in enough of a timely manner to adjust deployment of resources and tailor capability packets to that specific set of circumstances. These capabilities packages could also provide a general deterrence value by demonstrating an ability to counter threat lines of operations. The end result is a "menu" of options to prevent and defeat attacks that is comprehensive and comprehensible because it is expressed as a list of potential lines of operation against the threat and a list of specific capabilities required to succeed and overcome inherent challenges in HLD / HLS planning.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. CASE STUDIES: THE ADAPTABILITY OF A CAPABILITIES-BASED CONTINGENCY METHODOLOGY

After the terror of September 11th, the world has become a very dangerous place for soldiers on the front lines in the War on Terror and for first responders protecting the homefront. The *National Strategy for Combating Terrorism* recognized this new threat environment of terrorism, the "Axis of Evil," and the proliferation of Weapons of Mass Destruction (WMD) by stating, "The struggle against international terrorism is different from any other war in our history. We will not triumph solely or even primarily through military might."[41] In this new threat environment, military commands inside the US and even fire fighters and police have seen the need to develop plans and capabilities to address terrorism. "Within a few hours [on September 11th], the threats to our world had become exponentially more complex," the New York City Fire Commissioner concluded in the *FDNY Strategic Plan 2004-2005*, "the Fire Department, in turn, needed to adapt."[42]

The challenge for Homeland Defense and Homeland Security organizations is uncertainty as what to adapt to, with the threat being too ambiguous and diverse to clarify needed changes. In expressing the variety of threats facing the US, the *National Strategy for Homeland Security* (NSHLS) states, "Homeland security is focused on terrorism in the United States…Terrorists can be U.S. citizens or foreigners, acting in concert with others, on their own, or on behalf of a hostile state."[43] For military planners at United States Northern Command, counter-terrorism planners at the Department of Homeland Security (DHS), and strategic planners in police and fire departments, there are many questions: What exactly is the threat? What part of this threat is our responsibility? What capabilities will we need to detect and to stop these threats? The next concern is often the perplexing question: "how do I explain this plan to my boss?" To address these crucial questions, all agencies involved in Homeland Defense and Homeland Security should adopt a process to express which threats they must counter and what possible threat capabilities are involved.

---

41 *National Strategy for Combating Terrorism* (Government Printing Office, February 2003), 1.

42 Fire Department of New York City, *FDNY Strategic Plan 2004-2005* (New York City Fire Department, January 1, 2004), ii.

43 *National Strategy for Homeland Security* (Government Printing Office, July 2002), 2.

This chapter will address practical case study examples of HLS and HLD planning by demonstrating how two different agencies, one military and one non-military could adapt and adopt the proposed capabilities-based approach to contingency planning explained in the last chapter. The first case study will illustrate how military planners at the naval component of US Northern Command could use capabilities-based planning for a maritime HLD campaign plan. The second case study will reveal how non-military planners at a HLS agency such as the New York City Fire Department could use this capabilities-based planning approach to build a contingency plan for protecting their city. By showing how this approach can be utilized by both Homeland Defense (HLD) and Homeland Security (HLS) organizations, the flexibility and adaptability of capabilities-based planning will be demonstrated.

These case studies will reinforce how the "menu" approach of capabilities-based planning provides more flexibility than any threat-based or scenario-based alternatives for Homeland Defense and Homeland Security contingency planning. The requirement for this adaptability and flexibility in planning and resourcing was demonstrated when the *National Strategy for Homeland Security* stressed having "Foster Flexibility" as a guiding principle for Homeland Security.[44] These two case studies will show that very diverse agencies can use a capabilities-based approach to planning to define and codify amorphous threats and develop a list of required capabilities, authorities, and policies to counter anticipated terrorist actions while being inherently flexible to changes in their threat environment.

A. HOMELAND DEFENSE CASE STUDY: US NAVAL COMPONENT OF US NORTHERN COMMAND

The most important purpose and highest priority for the Department of Defense (DOD) is the defense of the Homeland against external threats and foreign aggression. In this core mission, DOD is responsible for Homeland Defense (HLD) which is defined as, "the protection of US sovereignty, territory, domestic population, and critical

44 U.S. Department of Homeland Security. *National Strategy for Homeland Security (NSHLS)*, July 2002 (Washington, DC.: US Government Printing Office, 2002), 4.

infrastructure against external threats and aggression."[45] While DOD requires capabilities to detect and defeat external threats and aggression anywhere in the world, DOD's goal will continue to be to deter and defeat threats as far from the Homeland as possible. Should deterrence fail, DOD requires a defense that is proactive, externally focused, and conducted in depth beginning at the source of the threat. The transit of threats to the Homeland from their source to their target presents DOD a series of opportunities to detect, deter, prevent, or defeat threat attacks and avoid the requirement to mitigate their effects. This layered defense approach to Homeland Defense includes a maritime defense pillar that protects US coastline and territorial waters from external threats including transnational terrorism.

The military organization responsible for the mission of maritime defense is US Naval Component of US Northern Command called US Navy North or "NAVNORTH." NAVNORTH is a 4-star Navy headquarters in Norfolk, Virginia. The NAVNORTH commander is dual-hatted as the Combined Fleet Forces Commander and in this role is in charge of training all US Navy crews and units assigned to ports in the continental US. The primary mission of NAVNORTH is Maritime Defense, defined as Homeland Defense operations taken to detect, deter, defeat, or nullify maritime threats against US territory, domestic population and infrastructure. While a full-scale maritime invasion of the homeland is unlikely, maritime forces under NAVNORTH's command may be employed to conduct offensive Homeland Defense operations when directed by the President and active and passive defenses in depth operations to deter and counter maritime attacks within US territorial waters. As the designated Joint Force Maritime Component Command for USNORTHCOM and the lead operational headquarters for Maritime Homeland Defense (where DOD is the lead federal agency), NAVNORTH also coordinates operations with the US Coast Guard (USCG) who is the lead operational agency for Maritime Homeland Security (with DHS as the lead federal agency) and port security.

[45] Definitions for Homeland Defense mission sets are from the final coordination draft of Joint Pub 3.26 *Joint Doctrine for Homeland Security*, dated 26 March 2004.

One of the main challenges facing NAVNORTH is the need for formal contingency planning against irregular maritime threats. After decades of threat-based planning against known navies of hostile nation-states, US Navy planners are now faced with planning against asymmetric threats. Existing contingency planning processes are proving ineffective because expected actions of these terrorist threat actors are vague and cannot be templated. With a wide diversity of potential attack scenarios, these planners and the leadership at NAVNORTH cannot do a scenario-based approach to maritime defense planning. The capabilities-based process may solve this challenge by providing the methodology to conduct a formal threat assessment based on threat capabilities and develop counters to each possible threat line of operation in the maritime domain.

An example of a simplified (and notional) capabilities-based threat assessment that NAVNORTH could plan for includes the transnational maritime attack threat line of operation in Figure 14. This notional line of operation for the threat would be built to include all unconventional asymmetric maritime threats aimed at the US Homeland, but tailored for the responsibility and role of NAVNORTH and the mission of maritime HLD. While each numbered capability point is subject to challenge and dissection by NAVNORTH and USNORTHCOM intelligence analysts and leadership, the holistic nature of the threat and what needs to be countered are graphically represented and easily explained. Intelligence on various threat actors would determine the most likely threat threshold as seen by the red diamond depicted at capability D6: “Multiple / coordinated hijack ships for kinetic attack with intelligence warning.” This threshold could tell the operational planners the magnitude of anticipated threat and which threat capabilities (D1 – D6) must be planned to counter and well as other potential maritime threat capabilities that, while less likely, are still a possible method of attack (D7 – D10). The “transnational maritime attack” line of operation (if conducted with actual intelligence available) could provide a product that would answer questions on the threat while being flexible to changing conditions on threat actors, intent, and capabilities.

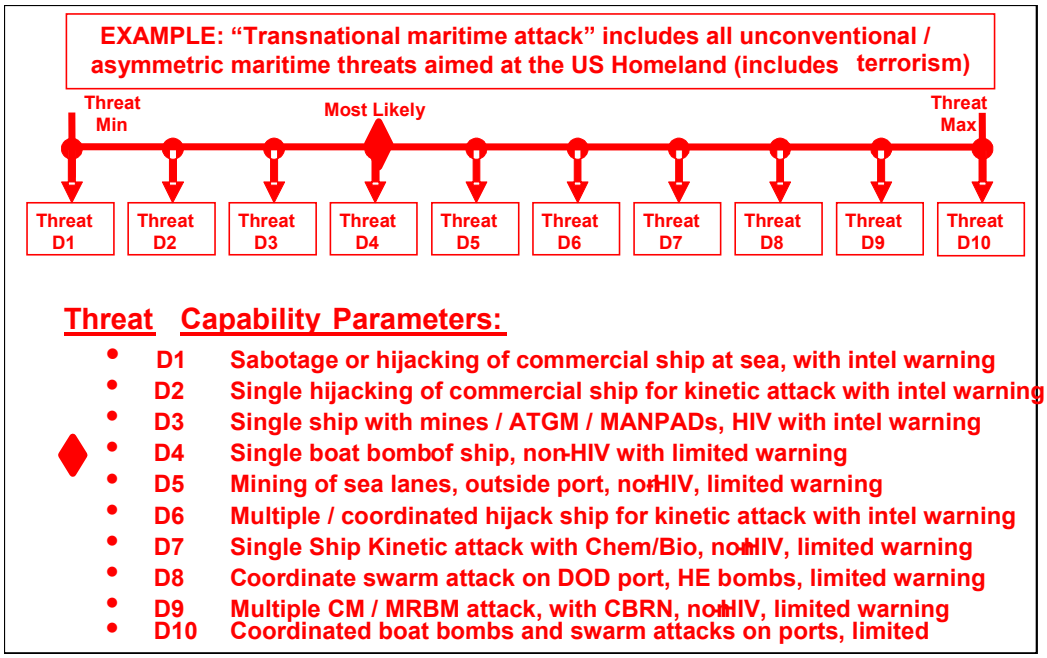

Figure 15. Capabilities-Based HLD Threat Assessments (Illustrative Purpose Only).

Using a capabilities-based threat assessment, maritime planners at NAVNORTH would then develop and validate plans and designate resources to counter each predicted threat capability. For example, for threat capability D-6 "Multiple / coordinated hijack ships for kinetic attack with intelligence warning," maritime planners could develop options for a Capability Force Package. This package could include required forces and resources to detect and characterize this threat and for both defense operations and offensive maritime intercept operations that could defeat any such threat attack. To develop these options, NAVNORTH planners would involve planners from various aspects of naval services to address the simple question "what can your command do to detect and defeat multiple and coordinated hijack ships the threat would use for kinetics attacks if you had some warning?"

The NAVNORTH Capability Force Package for threat capability D-6 emerge would integrate and synergize forces and operations from the tactical units and support agencies that could execute contingency operations for NAVNORTH. For example, naval aviation planners in the two fleet headquarters under NAVORTH would develop reconnaissance plans to detect and track high interest vessels and identify resource

requirements of P-3 surveillance aircraft and reconnaissance helicopters and supporting ships. Planners from 2nd and 3rd Fleet Headquarters could also answer the "what could you do" question by developing a concept of operation for Maritime Intercept Operations that identifies required combinations of specific ship types and supporting aviation platforms. In this manner, each possible contributor to the contingency mission (Marine Forces, Anti-Terrorism agencies, intelligence fusion centers, special operations planners, etc.) identifies options for needed capabilities, specifies forces and resource requirements, and identifies required enablers to utilize capabilities such as communication networks, logistical needs, and draft rules of engagement. Additionally, specialized capabilities that could be required such as mine detection platforms are identified and integrated into the Capability Package. Once each threat capability is addressed, a menu of options is developed for Capability Packages to detect, deter, and if necessary defeat transnational maritime attacks.

When the menu of options is expressed to senior decision-makers at NAVORTH, they can make informed decisions on risk versus resources trade-offs. In this example, the limited number of specialized P-3 surveillance aircraft and global demands for this platform could lead to decisions on the appropriate number to request for maritime defense – but only if the threat, required capabilities, possible mitigation substitutions, and the impact of any shortfalls on the mission are understood by decision-makers. Additionally, for any identified shortfalls in existing capability such as aerial detection of nuclear material, NAVNORTH can pass this requirement to USNORTHCOM and the US Navy to develop and field new capabilities and devote resources for more effective responses in the future.

In this case study, the end result of this process is a comprehensive and comprehensible Capability Force Package for an anticipated threat attack method like "multiple and coordinated hijack ships for kinetic attacks." Once each threat capability and threat line of operation has been addressed, NAVNORTH could share the resulting plan and force list with the fleet and task force headquarters that would be executing the plan. This would allow the capabilities-based plan to form the basis of exercises and wargames to validate and refine contingency plans and force packages. Including the threat capability D-6 and draft countering Capability Force Package D-6 into a tabletop

involving senior leaders at NAVNORTH and 2nd and 3rd Fleets would better prepare the entire command for this contingency. Each level of the maritime defense architecture would now have a formal and shared mechanism to link risk management, resource allocation, and exercises to continually evolve more effective plans to counter possible threat attacks. This case study shows how Homeland Defense planning by military organizations could be improved with the introduction of a capabilities-based planning process.

B. HOMELAND SECURITY CASE STUDY: NEW YORK CITY FIRE DEPARTMENT

While Homeland Defense is the purview of a limited number of Federal military commands, Homeland Security is a core mission of security, response, and law enforcement agencies at federal, state, and local levels. The *National Strategy for Homeland Security* defines HLS as a "concerted national effort to prevent terrorist attacks…" where the "concerted national effort" is based on "the principles of shared responsibility and partnership" among various Federal, state, and local agencies and with the American people.[46] The diverse and ambiguous nature of the terrorist threat is also a problem for agencies responsible for HLS, especially for security and law enforcement staff responsible for contingency planning in such a difficult environment. This planning and resource forecasting task is made all the more challenging because it is an activity that must be effectively conducted, and coordinated, at every level of government and by diverse agencies.

While the civilian Homeland Security community does not have a requirement for "campaign plans" like military commands such as NAVNORTH, these organizations have the equivalent function of contingency planning under the concept of "preparedness." The *National Response Plan* recognizes the vital nature of pre-event or pre-incident planning and defines this key function as:

> ***Preparedness***: The range of deliberate, critical tasks and activities necessary to build, sustain, and improve the operational capability to prevent, protect against, respond to, and recover from domestic incidents. Preparedness is a continuous process. Preparedness involves efforts at all

[46] *National Strategy for Homeland Security* (Government Printing Office, July 2002), 2.

> levels of government and between government and private sector and nongovernmental organizations to identify threats, determine vulnerabilities, and identify required resources.[47]

This preparedness function serves the traditional purpose of contingency planning by providing information, analysis, and recommendations to senior decision-makers to assist in the vision and expression of potential courses of action to meet future crises. The problem facing various organizations with Homeland Security responsibilities is the need to develop contingency plans to utilize existing capabilities in an effective manner against a thinking terrorist opponent who seeks surprise and shock. The true test of preparedness is whether the agency is ready and able to generate effective actions at the right time and place.

To examine how HLS preparedness planning could be done effectively with a capabilities-based approach, the New York City (NYC) Fire Department will form a second case study. This large organization faces a broad range of possible terrorism-related contingencies. The mission of the Fire Department of New York City (FDNY) includes preparedness and responding to terrorist events and reads, "as first responders to fires, public safety and medical emergencies, disasters and terrorist acts, the FDNY protects the lives and property of New York City residents and visitors."[48] Given the size of New York City and the enormous amount of commerce involved, this is a challenging task even for an emergency response organization numbering over eleven thousand fire fighters, twenty-five hundred paramedics and over a thousand support personnel. The FDNY leadership has expressed a need to "adapt" to a current and future environment that includes a complex threat of terrorism as the main difficulty facing the FDNY.[49]

To successfully adjust to the threat environment, a large and complex organization like the NYC Fire Department requires effective budgetary and contingency planning in order to meet current and future requirements of its many vital, yet diverse, missions. For the NYC Fire Department, contingency planning is conducted by the

---

[47] U.S. Department of Homeland Security. *National Response Plan* (December 2004), 71.

[48] Fire Department of New York City, *FDNY Strategic Plan 2004-2005* (New York City Fire Department, January 1, 2004), i.

[49] Fire Department of New York City, *FDNY Strategic Plan 2004-2005* (New York City Fire Department, January 1, 2004), ii.

Planning and Strategy unit inside the Department's Bureau of Operations. Once a team of experienced personnel are assigned to a planning task, a plan is developed with input from specialists and staffed to the Chief of Department, the Chief of the Bureau of Operations, and various other Senior Staff Chiefs before being sent to units to test and implement.[50] While appearing to be a formal process on paper, much of the actual planning has been traditionally done informally with a team from various safety, hazardous material, special operations, fire tactics, and medical rescue units meeting to address specific problems existing plans fail to address. This ad hoc process faces problems in both developing effective plans and in efficiently testing and implementing these plans. To be effective in this preparedness task, all these diverse capabilities and agencies require a synergizing planning process to coordinate preparedness and contingency planning.

To address this need, the *FDNY Strategic Plan 2004-2005* establishes a new standard for contingency planning with the key goal to enhance preparedness planning to address new threats and complex, long-term challenges. To accomplish this new focus on planning, the NYC Fire Department recently established a "Center for Terrorism and Disaster Preparedness" inside the Bureau of Operations. This center is the focal point for planning teams of experts established to develop, staff, approve, and recommend implementation of new plans. The challenge facing these traditional and new agencies is how to best prepare for terrorist events: i.e., how should the FDNY respond to a series of truck bombs exploding all across the city? Adopting a capabilities-based planning approach may help solve this problem by providing a clear method of assessing potential threat capabilities and developing a menu of FDNY capability packages to counter potential terrorist attacks and Homeland Security incidents.

A capabilities-based approach to threat assessment could work for HLS-type threats where agency responsibilities overlap. An example of a simplified (and notional) capabilities-based HLS threat assessment conducted by the FDNY Center for Terrorism and Disaster Preparedness can be seen in the transnational threat line of operation

[50] This background on contingency planning within the NYC Fire Department came from Ted Jankowski, Battalion Fire Chief, Bronx Division, and Executive Officer, Safety Command, New York City Fire Department.

involving New York City depicted in Figure 15. As this simplified assessment portrays, ten threat capabilities are determined to be the potential "how" the enemy might attack and the seven lowest magnitude capabilities (N1 – N7) are determined to be the most likely. This threshold "red diamond" of assessed probability would be adjusted by the FDNY based on intelligence "chatter" or perceived changes in vulnerabilities (for example, during a NYC special event). While focusing preparedness planners on the most likely threat, this capabilities-based assessment also depicts other, less-likely threats (N8-N10) that must be addressed in contingency planning due to their greater magnitude and potential impact. While greatly oversimplified, these example "red lines" show enough assessment of the threat that planners can identify and develop defensive lines of operation and capabilities needed to counter these threats.

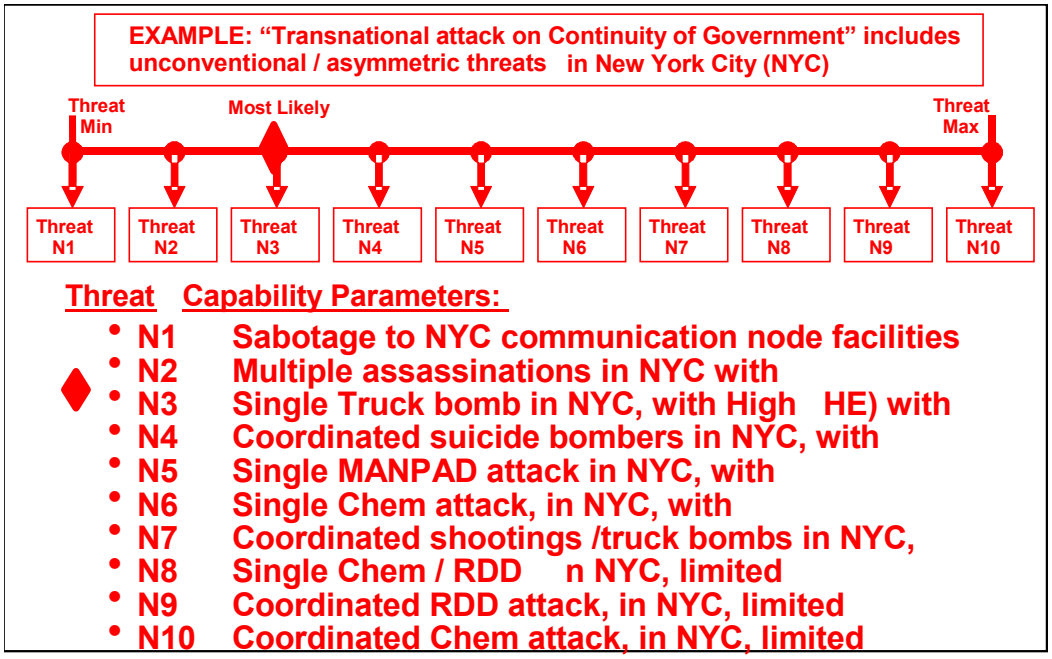

Figure 16. A Capabilities-Based HLS Threat Assessments (Illustrative Purpose Only).

Using a capabilities-based threat assessment, FDNY preparedness planners in the Center for Terrorism and Disaster Preparedness can develop plans and resources to counter each predicted threat capability. An example is the potential threat simplified as N-7: "coordinated shootings and truck bombs in NYC with limited warning." In order for FDNY planners to develop a counter Capability Force Package options, planners from

various agencies inside the FDNY would simply answer the question "what can we do about N-7." In a conference of representatives from the Emergency Management Service (EMS) Divisions, the Fire Operations Boro Commands, and specialized agencies like the Intergovernmental Affairs and Management Initiatives Agency would identify capabilities and operational concepts that could be employed to defeat and mitigate this type of terrorist attack. This process would also allow these planners to identify and coordinate resources and enablers required to operate during this type of attack by addressing what steps should be done and by whom in the event of a warning of a "coordinated shootings and truck bombs in NYC with limited warning."

The FDNY HLS Capability Package for threat capability N-7 that could emerge would integrate and synergize forces and operations from the tactical units and support agencies that could execute contingency operations for the Fire Commissioner. For example, Fire Battalion Commanders in threatened Boro Divisions could implement asset dispersal plans and coordinate truck bomb specific procedures with the NYC Police Department. Planners from EMS Division Headquarters could also answer the "what could you do" question by developing a concept of operation for truck bombs that identifies required combinations of specific EMS vehicle types and supporting personnel. Each possible contributor to the contingency mission (FDNY Operational Units, Special Operations Command, Logistics and Support, the Bureau of Fire Prevention, etc.) identifies options for needed capabilities, specifies units and resource requirements, and identifies required enablers to utilize capabilities such as communication networks, logistical needs, and security reporting procedures. Additionally, specific specialized capabilities that could be required such as explosive disposal teams are identified and integrated into the Capability Package. Once each threat capability is addressed, a menu of options is developed for HLS Capability Packages to detect, deter, and if necessary mitigate coordinated shooting and truck bomb attacks inside NYC.

When this menu of options is expressed to senior decision-makers (the Chief of Operations and the Chief of Department) and then to the Fire Commissioner, they can make informed decisions can be made on risk versus resources trade-offs. In this example, the limited number of specialized bomb disposal teams and possible false alarms demands for this platform could lead to decisions on the appropriate number to

train for vehicle-borne explosive devices – but only if the threat, required capabilities, possible mitigation substitutions, and the impact of any shortfalls on the mission are understood by decision-makers. Additionally, for any identified shortfalls in existing capability such as portable incident command and communication vehicles, the Center for Terrorism and Disaster Preparedness can pass this requirement to the Chief of Department and Chief of Operations who would forward this to the department's Bureau of technology and Communications Bureau develop and field new communications capabilities and devote resources for more effective multiple incident responses in the future.

A FDNY preparedness plan with identified capability packages could also provide a mechanism to validate capability requirements through experimentation. The Chief in Charge of the FDNY Bureau of Training could use pre-planned packages for "coordinated shootings and truck bombs in NYC with limited warning" as a tabletop with the senior leadership of the department to validate options and better prepare for this response. Each of the Boro Divisions could also exercise their own developed response packages for the contingency N-7 to overcome problems, refine and coordinate plans, and identify capability shortfalls within their Boro Fire Battalions and EMS Divisions. For any such identified capability shortfalls, NYC elected officials can devote additional resources for more effective responses if the risk versus resources tradeoffs are formalized and presented in a comprehendible manner.

This case study shows how the FDNY could use capabilities-based planning to overcome HLS challenges in preparedness planning. The FDNY leadership has already recognized the need for such a comprehensive and easy-to-understand process. "Since the September 11th attack on the World Trade Center, we have been reassessing our missions and strategic goals," the New York City Fire Chief of Department Frank C. Cruthers wrote in the *FDNY Strategic Plan 2004-2005*, "The attacks have given us a new sense of urgency to broaden our response capabilities to include terrorism preparedness."[51] To meet this test, a capabilities-based planning approach could provide a formal and shared

[51] Fire Department of New York City, *FDNY Strategic Plan 2004-2005* (New York City Fire Department, January 1, 2004), iii.

mechanism to link risk management, resource allocation, and response exercises to validate choices made during preparedness planning.

C. CASE STUDY IMPLICATION

As these two case studies demonstrate, a capabilities-based approach to threat assessment may serve both Homeland Defense and Homeland Security organizations well by facilitating capabilities-based planning and preventing gaps in defense and preparedness capabilities. This innovative approach toward developing formalized plans for HLD and HLS may be the best approach to what looks more and more like a long war versus the threat of terrorism with shrinking distances often placing local and state authorities on the front lines. Looking at these notional Homeland Defense and Homeland Security case studies, a capabilities-based approach to contingency planning is inherently flexible and has the additional advantage of facilitating the planning process by ease of comprehension and explanation. Because of the simple nature of this method of threat assessment and capability package development, this capabilities-based approach to planning can be adapted and adopted in part or in total by any organization involved in countering terrorist threats.

The flexibility and adaptability inherent in a capabilities-based approach to planning is also true vertically within organizations. From strategic headquarters to operational agencies down to tactical departments and units, all levels within an organization can use the same planning process to formalize the passing of threat assessments, operational plans, and resourcing decisions up and down organizational leadership. Examples will show how this is true for both HLD and HLS. For Homeland Defense, NAVNORTH could complete their plan and assign responsibility for a specific threat capability to an operational headquarters like Third Fleet to counter capability N4. Then, within Third Fleet, the operational agency can further subdivide response responsibilities to specific ships and task forces. This would allow planners at all levels to share a common language for addressing threats and developing response packages that then could be passed to exercise planners to better integrate planning with exercises at every level of a military command.

A similar process of vertical integration can work for Homeland Security organizations. The Emergency Operations Center for New York City can task the FDNY to develop plans and capabilities for specific threat capabilities. Inside the FDNY, the Center for Terrorism and Disaster Preparedness could then task fire battalions and special agencies to address specific threat actions or incident types. In this manner, each part of the organization, from the Fire Commissioner to a specific fire station or EMS unit, would be integrated in a single preparedness plan. This capabilities-based process can also assist HLS preparedness by linking contingency planning to emergency exercises wherein the response for threat capabilities is formalized and practiced at each level. As a result, this method of preparedness planning could link FDNY, NYPD, and hospitals in NYC by sharing a common threat assessment and contingency planning process.

This conceptual approach to contingency planning could provide an explicit linkage process to HLD and HLS arena for contingency planning by allowing for a sharing of planning language and methods. The existing overlap of HLS and HLD threats mean both military and civilian agencies need to formally address "what could we do about threat capability X" in some integrated fashion in order to develop a menu for decision-makers. In some cases, responding with a military capability to a specific threat or threat group will be appropriate – and in some cases it will clearly not be appropriate. As the *National Security Strategy* concludes, "To defeat this [terrorist] threat we must make use of every tool in our arsenal – military power, better homeland defense, law enforcement, intelligence, and vigorous efforts to cut of terrorist financing."[52] Ambiguity will continually challenge Homeland Defense and Homeland Security planning in the current strategic environment by raising the question "what is the threat" when planning to confront enemies whose composition and intent are unprecedented. The solution to this challenge demonstrated in these case studies can help bridge this seam in planning a national response to the threat of terrorism.

[52] *National Security Strategy of the United States* (Government Printing Office, September 2002), i.

V. CONCLUSION

To address the challenges of the post-9/11 world, Secretary of Defense Donald Rumsfeld described his way ahead by stating that the leadership of DOD had, "decided to move away from the old 'threat-based' strategy that had dominated our country's defense planning for nearly half a century and adopt a new 'capabilities-based' approach -- one that focuses less on who might threaten us, or where, and more on how we might be threatened and what is needed to deter and defend against such threats."53 By adopting this approach both inside and outside DOD, capabilities-based planning would provide senior military decision-makers with an understandable process that has the inherent flexibility to address both Homeland Defense and Homeland Security contingency planning. Bracketing potential hostile capacities with assumptions of likelihood facilitates narrowing planning into manageable (and often affordable and acceptable) realms. Amorphous threats such as terrorism can be defined in this way and codified to enable planners to develop a list of required capabilities, authorities, and policies to counter anticipated enemy actions while being inherently flexible to changes in the strategic threat environment.

A. RECOMMENDATIONS

- **DOD should halt the use of a traditional threat-based planning process for Homeland Defense contingency planning**

While traditional threat-based planning methods and "capabilities-based planning" are two equally valid but mutually exclusive planning methodologies, traditional military planning only works when you have - and are planning to have - the initiative. Capabilities-based planning on the other hand almost inherently assumes you do NOT have the initiative and plans on countering threat capabilities and threat actions - not actually determining what to do in the absence of a threat action. Capabilities-based planning can thus be described as a "countering" methodology for contingency planning

53 Donald H. Rumsfeld, "Transforming the Military," *Foreign Affairs* Volume 81, Number 3 (May/June 2002).

and may not be the most effective planning process in areas where the US government has the initiative. Both capabilities-based and threat-based approaches to planning have roles in current DOD planning, but traditional threat-based planning is really only appropriate for the overseas warfights and should not be applied to defense and security planning inside the US.

- **Both DOD and DHS should adopt a capabilities-based approach for threat assessments for Homeland Defense and Homeland Security planning**

As is required by the defensive mission of protecting the US Homeland, capabilities-based threat assessment allows a greater focus on the "how" and not the "who" of the threat. While the intelligence community will continue to seek hard information on threat groups and key leaders, much of the resulting intelligence data can too often cause over-reaction among defense and security planners unless each piece of data is integrated into a larger framework. The threat warnings in the months after 9/11 demonstrated this as nuclear powerplants, airports, ports, trains carrying chemicals, and various other targets became the focus of the day. This occurred despite the fact that multiple actors who had this capability could have attacked each of these on any day in multiple ways. Planners need to focus to identify and define the threat of a truck bomb for example; it matters little to defense and security planners which group actually recruited the driver and rented the truck. By using a capabilities-based approach to threat assessment, the question "who is the threat" is reworded as "what could the threat *DO*" to allow exploration of a much broader range of eventualities and give HLD or HLS planners a defined and detailed threat to plan against. This alone would be welcome in nearly all contingency discussions on protecting the Homeland against terrorist threats as a method to overcome challenges of uncertainty haunting current HLD and HLS planning efforts.

- **Both DOD and DHS should adopt a capabilities-based methodology for Homeland Defense and Homeland Security contingency planning**

Capabilities-based planning combines the strengths of the threat-based and scenario-based planning methods while maintaining flexibility. Because of the diffuse threat environment and the great probability of the enemy's use of surprise, Homeland Defense planning "requires identifying capabilities that U.S. military forces will need to deter and defeat adversaries who will rely on surprise, deception, and asymmetric warfare to achieve their objectives."[54] Matching means and methods against threat capabilities, capabilities-based planning is an effective approach to Homeland Defense planning for military planners and non-military Homeland Security planners in today's ambiguous strategic environment. This process can identify required tools and the required authorities and policies to utilize them. As the *National Security Strategy* concludes, "To defeat this [terrorist] threat we must make use of every tool in our arsenal – military power, better homeland defense, law enforcement, intelligence, and vigorous efforts to cut off terrorist financing."[55]

- **Both DOD and DHS should leverage a capabilities-based methodology to formalize linkages between planning and resourcing for Homeland Defense and Homeland Security contingency planning**

Each piece of new intelligence would further refine what threat capabilities exist and any "actionable intelligence" would trigger the execution of pre-planned defense and security capabilities with required resources already identified and enabled. Secretary of Defense Rumsfeld described this concept well when he wrote,

> It's like dealing with burglars: You cannot possibly know who wants to break into your home, or when. But you do know how they might try to get in. You know they might try to pick your lock, so you need a good, solid, dead bolt on your front door. You know they might try breaking through a window, so you need a good alarm. You know it is better to stop them before they get in, so you need a police force to patrol the

[54] Department of Defense, *Quadrennial Defense Review Report* (Government Printing Office, 30 September 2001), 14.

[55] *National Security Strategy of the United States* (Government Printing Office, September 2002), i.

> neighborhood and keep bad guys off the streets. And you know that a big German Shepherd doesn't hurt, either.[56]

While all this may seem common sense (as most quality planning is), a plan's effectiveness is limited by how comprehensive and comprehensible the resulting plans and briefings are - whether the plan is to stop burglar or terrorists.[57] The proposed capabilities-based planning method accomplishes this by producing a menu of options for decision-makers that is directly related to specific threat capabilities and linked to specific resources.

- **Both DOD and DHS should leverage a capabilities-based methodology to formalize linkages between planning and exercises for Homeland Defense and Homeland Security contingency planning**

Because the threat is not contingency-based but rather a steady state, HLD and HLS planning needs to be constantly cyclic and remove the clear distinction between planning and execution (see Figure 17). Key is to exercise and test the plan in a cyclic process. The first step must be the creation (or refinement) of an agreed-upon threat assessment that is understood. Next, planners build upon this to develop counters and produce a capabilities-based menu of response options. The third step is to allow the planning process to facilitate the key resources versus risks decisions by the organizational leadership. The final step in the planning cycle is to identify capability shortfalls that feed the resources requirement and budget cycle processes and link contingency planning with future budgeting. However, operational execution could interrupt this planning cycle and test the plans developed. If the plans are tested in real-world execution (or by exercises), these must be followed by a post-execution assessment that can be used to improve and refine contingency plans.

---

[56] Donald H. Rumsfeld, "Transforming the Military," *Foreign Affairs* Volume 81, Number 3 (May/June 2002).

[57] But if the main strength of the system is based on a "tool box" analogy, this is also the main weakness. One of the strongest criticisms of capabilities-based planning comes from a National War College paper written with the goal of exposing the "myth" of capabilities-based planning. A War College student asserts that pure capabilities-based planning would be like outfitting a toolbox with the latest and best tools but fails to answer, "how big of a toolbox should you build? How many of each tool do you need? How many of these tools need external support in getting to the job at hand?" Additionally, an inherent challenge emerges of how do you judge the effectiveness of each tool for a job you have not conducted yet. Jeffery B. Kendall, *Capabilities-Based Military Planning: A Myth*. National War College Paper, Doing National Military Strategy Seminar (National Defense University, 17 April 2002), 5.

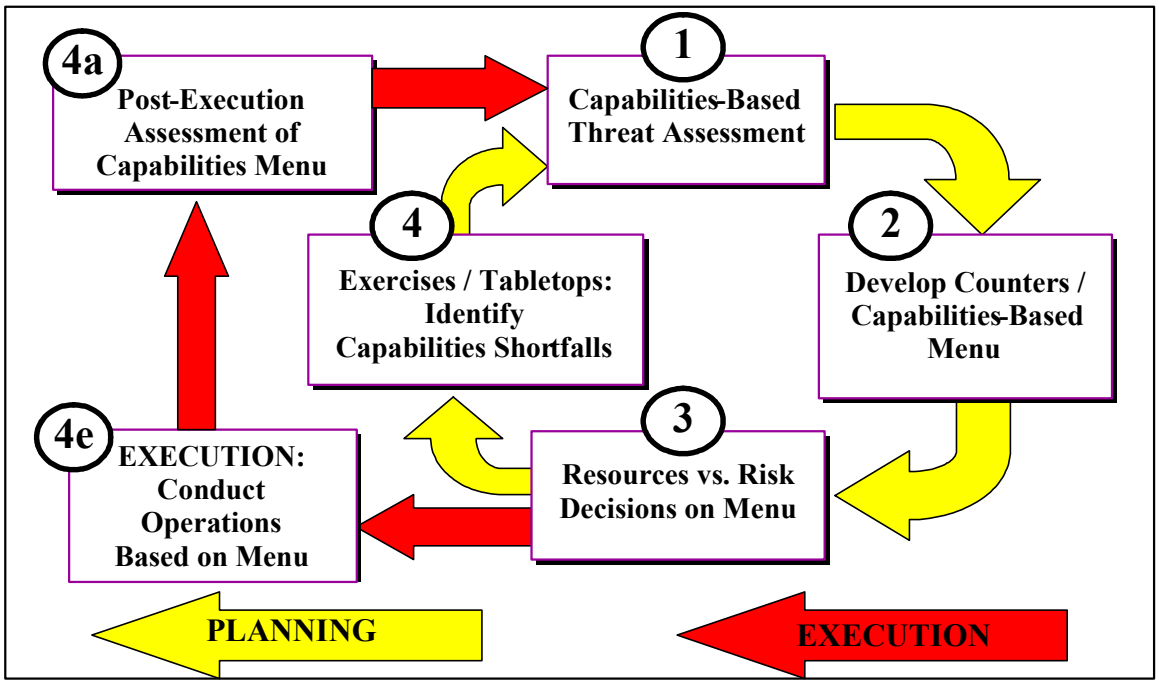

Figure 17. Capabilities-Based Planning and Execution Cycles.

- **Both DOD and DHS should leverage a capabilities-based methodology to increase senior decision-maker involvement in Homeland Defense and Homeland Security contingency planning**

One of the fundamental advantages of the capabilities-based planning process is the explicit nature of the planning process. In expressing the threat assessment and resulting capabilities menu, the planning process can be traced and each step explained. Assumptions and choices to be tested and challenged in order to constantly revise, update, and improve the contingency plan. This planning process has the ability to better integrate senior decision-makers in the process by presenting plans in a comprehensible format and allowing iterative involvement at every level of management and across different agencies and organizations. Once a framework or "menu" of these capabilities is identified, senior decision-makers will recommend for development and if required the use of military and security capabilities that best protect the United States. Capabilities-based planning can fulfill this requirement by formulating plans that can be expressed and adapted as both a menu of options and a rheostat of degrees of preventive response –

all dictated by changes in intelligence warning. This approach to contingency planning more than meets the overall DOD objective to overcome uncertainty with flexibility in planning.[58] The objective is that capabilities-based planning will produce living documents with options and branches that are fundamentally different from traditional contingency plans. This also can overcome concerns that existing contingency plans appear to be detailed rigid plans that fill volumes on the shelf but offer as the only decision for national leaders is to approve the execution and sit back and watch.

[58] According to current work on DOD Defense Planning Scenario development, "Capabilities-Based Planning is a method of Defense planning that examines a wide range of variability in factors, in order to achieve a broad portfolio of military capabilities that will perform robustly in an uncertain future environment." This unclassified quote is from a classified DOD briefing dated July 2003 from the Office of the Secretary of Defense that accompanied the staffing of the Defense Planning Scenarios.

LIST OF REFERENCES

U.S. GOVERNMENT AND DEPARTMENT OF DEFENSE PUBLICATIONS:

U.S. Department of Defense. *Quadrennial Defense Review Report,* 30 September 2001. Washington, DC.: Government Printing Office, 2001.

U.S. Department of Defense. CJCSI 3170.01D, *Joint Capabilities Integration and Development System*, 12 March 2004. Washington, DC.: US Government Printing Office, 2004.

U.S. Department of Defense. CJCSM 3122.01, *Joint Operation Planning and Execution System (JOPES), Volume 1 (Planning Policies and Procedures)*, 14 July 2001. Washington, DC.: US Government Printing Office, 2001.

U.S. Department of Defense. "Adaptive Planning Study Draft Concept," briefing by OSD-Strategy, dated 13 January 2004 (Unclassified).

U.S. Department of Defense. *Defense Planning Guidance (DPG) 2004-2009* (U), May 2002. Washington, DC.: US Government Printing Office, 2002

U.S. Department of Defense. *Dept of Defense Transformation Planning Guidance* (TPG), April 2003. Washington, DC.: US Government Printing Office, 2003.

U.S. Department of Defense. *Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms*, 12 April 2001. Washington, DC.: US Government Printing Office, 2001.

U.S. Department of Defense. *Joint Publication 2-0: Doctrine for Intelligence Support to Joint Operations*, 09 March 2000. Washington, DC.: US Government Printing Office, 2000.

U.S. Department of Defense. *Joint Publication 3-26: Homeland Security*, Final Coordination Draft, 26 March 2004.

U.S. Department of Defense. *Joint Publication 5-0: Doctrine for Planning Joint Operations*, 13 April 1995. Washington, DC.: US Government Printing Office, 1995.

U.S. Department of Defense. *National Military Strategy*, 13 May 2004. Washington, DC.: Government Printing Office, 2004.

U.S. Department of Homeland Security. *National Response Plan*, December 2004.

Federal Bureau of Investigation, *Strategic Plan, 2004-2009*. Federal Bureau of Investigation; available from http://www.fbi.gov/publications/strategicplan /strategicplanfull.pdf; internet; accessed 12 August 2004.

GAO Report to U.S. Congress. *Homeland Defense: DOD Needs to Address the Structure of U. S. Forces for Domestic Military Missions*, July 2003. Washington, DC.: United States General Accounting Office, 2003.

Homeland Security Council, *Planning Scenarios: Created for Use in National, Federal, State, and Local Homeland Security Preparedness Activities*, July 2004 (For Official Use Only). Washington, DC., 2004.

U.S. Homeland Security Presidential Directive (HSPD) 5, *Management of Domestic Incidents*, 28 February 2003. Washington, DC.: US Government Printing Office, 2003.

National Military Strategic Plan for the War on Terrorism, October 2002. Washington, DC.: US Government Printing Office, 2002.

National Security Strategy of the United States of America, September 2002. Washington, DC.: US Government Printing Office, 2002.

National Strategy for Combating Terrorism (NSCbT), February 2003. Washington, DC.: US Government Printing Office, 2003.

U.S. Department of Homeland Security. *National Strategy for Homeland Security (NSHLS)*, July 2002. Washington, DC.: US Government Printing Office, 2002.

OTHER PUBLISHED SOURCES:

Alberts, David S. and Richard E. Hayes. Power to the Edge: Command…Control… in the Information Age. Washington, DC.: Command and Control Research Program, CCRP Publications, 2003.

Belanger, Micheline, and Adel Guitouni. *A Decision Support System for COA Selection*. Defense Research Establishment Valcarier; available from http://www.dodccrp.org/2000ICCRTS/cd/ papers/ Track5/049.pdf; internet; accessed 20 January 2004.

Campbell, Kurt M. and Michele A. Flournoy. To Prevail: An American Strategy for the Campaign Against Terrorism. Washington, DC: CSIS Press, 2001.

Courtney, James F. *Decision Making and Knowledge Management in Inquiring Organizations: Toward a new Decision-Making Paradigm for DSS.* ScienceDirect: Decision Support Systems; available from http://www.sciencedirect.com/science.html; internet. Decision Support Systems, Volume 31, Issue 1, May 2001, pages 17-38; accessed 23 January 2004.

Davis, Paul K., *New Challenges for Defense Planning: Rethinking How Much Is Enough.* Santa Monica, CA: RAND Corporation Publication MR-400-RC, 1994.

Davis, Paul K., *Analytic Architecture for Capabilities-Based Planning, Mission Systems Analysis, and Transformation.* Santa Monica, CA: RAND Corporation Publication MR 1513, 2002.

Fire Department of New York City, *FDNY Strategic Plan 2004-2005*. New York City Fire Department, January 1, 2004.

Harder, Robert J. and Howard Higley, *A Group Support System for Military Mission Analysis*. 36th Hawaii International Conference on Systems Science (2003); available from http://csdl.computer.org/comp/proceedings/hicss/2003.pdf; internet; accessed 20 January 2004.

Kahan, Jerome H., Tindal, Zavadil, Stephen W., The New US Strategic Framework and Capabilities-based Planning: Application to Strategic Force Planning, June 2003.

Kendall, Jeffery B., *Capabilities-Based Military Planning: A Myth*. National War College Paper, Doing National Military Strategy Seminar. National Defense University, 17 April 2002.

Killion, Thomas H. "Decision Making and the Levels of War," in *Military Review*, US Army Command and General Staff College, November – December 2000, pages 66-70.

McKinsey and Company, *Increasing FDNY's Preparedness.* August 20, 2002.

New Challenges, New Tools for Defense Decisionmaking. Stuart Johnson, Martin Libicki, and Gregory F. Treverton, editors. Santa Monica, CA: RAND Corporation Publication MR-1576-RC, 2003.

Potter, Richard E., R. Kelly Rainer, Jr., and Efraim Turban. Introduction to Information Technology. Hoboken, N.J.: John Wiley & Sons, 2003.

Powers, D. J. *A Brief History of Decision Support Systems*. DSSResources.com [journal on-line]; available from http://dssresources.com/history/dsshistory.html, version 2.8, May 31, 2003; internet; accessed 20 January 2004.

Rumsfeld, Donald H "Transforming the Military," in *Foreign Affairs* Volume 81, Number 3, May/June 2002.

Thompson, Katherine S., *Executive Research Project: The Role of the Military in Homeland Security.* Fort McNair, Washington, DC.: National Defense University, 2002.

Watson, Hugh J., George Houdeshel, and Rex Kelly Rainer, Jr. Building Executive Information Systems and other Decision Support Applications. Hoboken, N.J.: John Wiley & Sons, 1997.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California