Homeland Security Affairs

Volume I, Issue 1 2005 *Article* 5

Summer 2005

Building a Contingency Menu: Using Capabilities-Based Planning for Homeland Defense and Homeland Security

Thomas Goss*

*familygoss@aol.com

Building a Contingency Menu: Using Capabilities-Based Planning for Homeland Defense and Homeland Security

Thomas Goss

Abstract

Terrorist threat actors are both cunning and adaptive, relying on surprise to overcome security measures. For this reason, military and security planners must embrace a more flexible, comprehensive, and comprehensible approach to contingency planning – a method based on neither threats nor scenarios exclusively, but rather on integrating these two approaches into a planning process based on capabilities. Using the concepts of "lines of operation" and "capabilities" as dynamics to define and explain potential and likely interactions, the capabilities-based planning method proposed in this article produces a menu of options for decision-makers that are directly related to specific threat capabilities and linked to specific resources. The question "who is the threat?" is reworded as "what could the threat do?" allowing exploration of a much broader range of eventualities and giving Homeland Defense and Security planners a defined and detailed threat to plan against.

AUTHOR BIOGRAPHY: Lieutenant Colonel Thomas Goss is an active duty officer in the U.S. Army currently serving on the International Military Staff at the North Atlantic Treaty Organization (NATO) Headquarters in Brussels, Belgium. For the last four years, LTC Goss has been a Strategic Plans and Policy officer working on issues of Homeland Defense and Homeland Security while assigned to North American Aerospace Defense Command (NORAD) and U.S. Northern Command in Colorado Springs, Colorado. LTC Goss received a Ph.D. in History from Ohio State University and recently graduated from the Naval Postgraduate School with a master's degree in Homeland Security.

KEYWORDS: prevention, planning, capabilities, lines of operation, threat definition

INTRODUCTION: The Vital Task of Planning for the Worst

"Within a few hours [on September 11, 2001], the threats to our world had become exponentially more complex," the New York City Fire Commissioner concluded in the *FDNY Strategic Plan 2004-2005*, "[and] the Fire Department, in turn, needed to adapt."[1] The challenge for homeland defense and homeland security organizations is uncertainty as to what to adapt to, with a threat being too ambiguous and diverse to easily identify. 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? Because terrorist threat actors are both cunning and adaptive, relying on surprise to overcome security measures, military and security planners must embrace a more flexible, comprehensive, and comprehensible approach to contingency planning – a method based on neither threats nor scenarios exclusively, but rather on integrating these two approaches into a planning process based on capabilities.

The process of contingency planning and resource allocation poses one of the greatest current challenges for those responsible for protecting the United States 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 designating "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."[2] At this task, military and security planners have struggled to develop a comprehensive and comprehensible planning system using existing approaches of traditional threat-based planning that focus on the "who," and scenario-based planning 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 thus frame required capabilities and overcome uncertainty concerning the threat.

PROBLEMS WITH CURRENT PLANNING METHODOLOGIES

The *National Security Strategy* identifies the vital function of having a formal and deliberate process of threat assessment, yet such process has yet to gain wide acceptance. Conceptually, there are three fundamental approaches to conducting a threat assessment, focusing on the "who," the "what," and the "how" of the threat. In a traditional threat assessment, analysts address the "who" of the threat: the threat actor(s), their "order of battle," and their most likely courses of action. The second conceptual approach looks 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 planners should address through threat scenarios.

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 course-of-action, most dangerous course-of-action, values, and critical vulnerabilities."[3] Based on this threat assessment and strategic guidance, planners develop a single course of action with branches and sequels. This traditional

planning process results in decision-makers selecting a single contingency plan with a "throw the switch" type of action. Traditional military planning process can thus be seen as a single decision chain, which was effective 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.

However appropriate this traditional approach is for a threat like the North Korean military, threat-based planning produces only guesses in the face of state-sponsored and non-state threat actors that the U.S. faces currently. This is due, in turn, to such things as a dearth of intelligence on Al Qaeda's organizational structure and operational capabilities. Without knowing how many "cells" are operating, how they receive operational guidance, and where specifically they plan to strike, planners have little on which to build plans. While intelligence successes in the global war or terrorism have been filling in the blanks on many such questions, the absence of a template will continue to frustrate those who seek to apply a traditional "who" approach to the unprecedented threats to the United States. 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" or determine courses of action.

After 9/11, many homeland security 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, and shows the advantages of this method of planning: it is simple to execute and modifiable based on the scenarios selected. These "what if" contingency plans have the additional 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 produces plans only for the contingency scenarios selected. These problems 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 known as the "Nine Scenarios." The goal of this planning exercise was to clarify DOD responsibilities during the establishment of the DHS. During 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, and 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. This is precisely what planners are told to avoid: "fighting the scenario."

The DHS recently attempted to overcome this challenge by formalizing a set of standard threat scenarios. This form of "universal threat" planning is designed to be the foundation for the

development of all "national preparedness standards from which homeland security capabilities can be measured."[4] 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 "for domestic incident preparedness to proceed through a capabilities-based approach."[5]

This effort has run into resistance from homeland security planners who claim that "one size does *not* fit all." The 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.[6] City planners and decision-makers are quick to point out that each city is in fact unique in its infrastructure, assets, resources, and vulnerability. The challenge for any scenario-based approach is to be able to plan with certainty that the scenarios developed will be the scenarios faced. That certainty is a rare and perishable commodity in the diverse planning community that addresses the multifaceted and ambiguous threats to the U.S. Homeland.

Therefore, neither "threat-based" nor "scenario-based" planning will work effectively for homeland defense or homeland security planning because the asymmetric threat cannot be used as a template.[7] 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:

- Threat-based planning is very susceptible to threat deception, causing the U.S. 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 the unconventional 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.[8]

The memories of 9/11 and the fears of unprecedented terrorist capabilities combine with these uncertainties to drive homeland defense and homeland security planners to search for a planning process that avoids these pitfalls.

DEVELOPING A CAPABILITIES-BASED PLANNING METHODOLOGY

To address the perceived growing complexity of the global security situation for the United States, the Department of Defense (DOD) is advocating "capabilities-based" defense planning to achieve a broad portfolio of military capabilities that will perform robustly in uncertain future environments.[9] As first formalized in the 2001 DOD *Quadrennial Defense Review*, a capabilities-based approach "focuses more on how an adversary might fight rather than specifically whom the adversary might be or where a war might occur."[10] To accomplish this broad goal, DOD planning 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." 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 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, who 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."[11] 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.[12] This helps planners to define capabilities needed rather than individual numerical solutions to narrowly defined, highly scripted individual 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 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 strike means, capacity, and likelihood of all potentially hostile actors, with an emphasis on recasting intelligence uncertainty into a modular "menu" of potential threat capabilities. This planning process results in a solution framework emphasizing "building blocks" of capabilities that could be tailored to meet persistent general threats or a specific emerging threat.[13] By bracketing potential hostile capacities with assumptions of likelihood, planners can define and codify amorphous threats, develop a list of required capabilities and required authorities and policies to counter anticipated enemy actions, and retain flexibility in response to changes in the strategic threat environment. Each new piece of new intelligence further refines what threat capabilities exist and any "actionable intelligence" triggers the execution of pre-planned defense and security capabilities already identified and enabled.

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 clear to senior decision-makers. This ensures both senior leader involvement and the ability to make sound choices. By leveraging senior leader involvement, a 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.

DEVELOPING A CAPABILITIES-BASED THREAT ASSESSMENT

A new conceptual approach that combines the strengths of threat-based and scenario-based thinking needs to be found to structure and assess threats in homeland security and 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 interactions. As opposed to the spatial or temporal divisions of the battle space by borders, or 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."[14] 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)."[15] 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 (such as tactics and weapon performance). For this article, a capability is defined as the ability to perform a specified task 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.

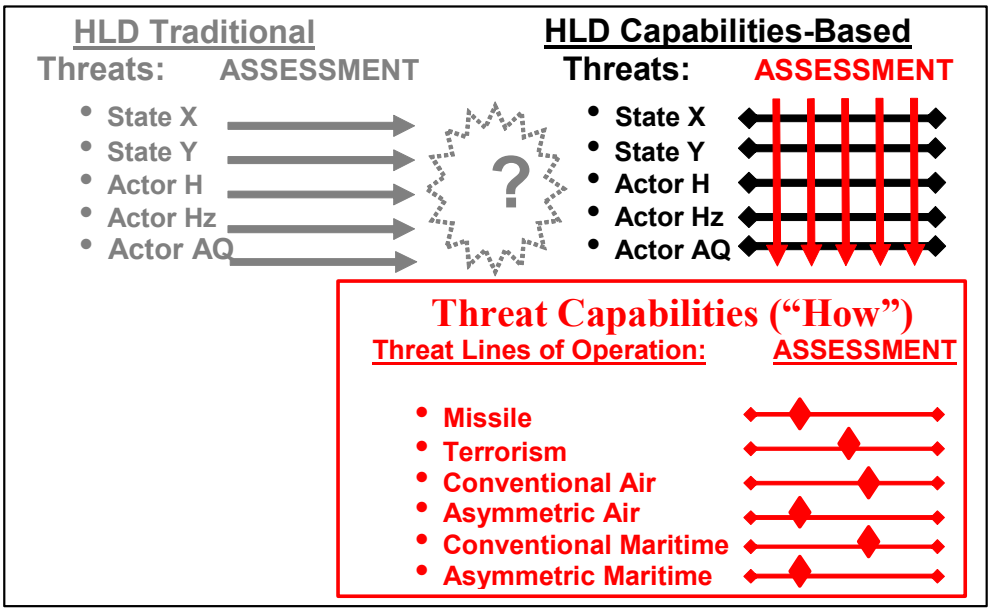

Figure 1
A Capabilities-Based Approach to Threat Assessment

In terms of identifying 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 1). For example, with multiple actors possessing the means and

the will to conduct terrorism in the U.S. Homeland, the focus of assessment is not Al Qaeda, but any potential terrorist group; i.e., 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 Qaeda will strike next, but how 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 U.S. (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 homeland defense planning.

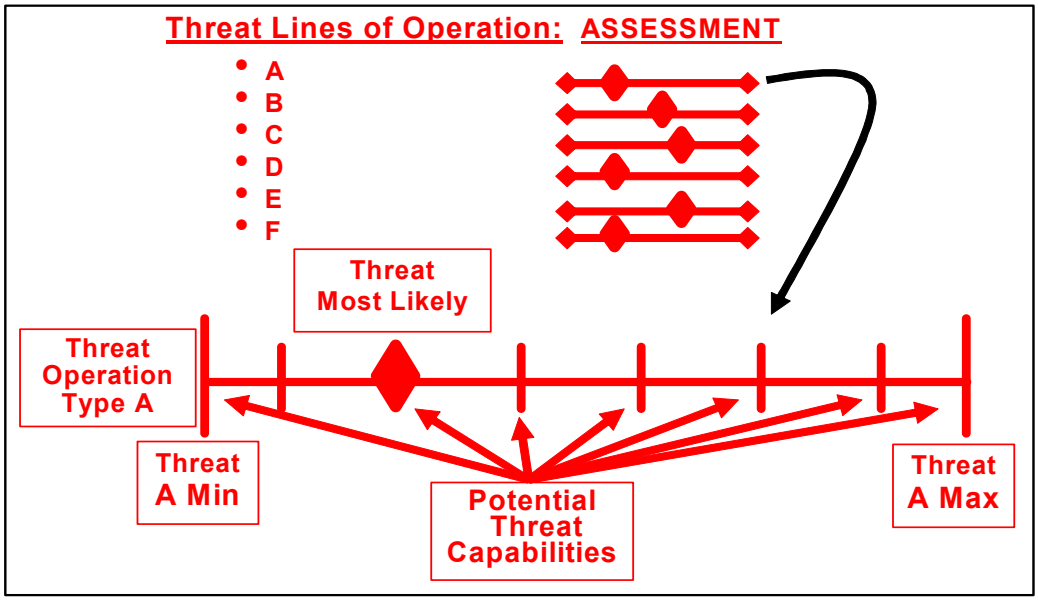

Figure 2
Developing Threat Lines of Operation and Threat Capabilities

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 poses to the U.S. Homeland (see Figure 2). 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 homeland defense capability). For example, the minimum threat to the U.S. 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 China,

France, Great Britain, India, Israel, North Korea, Pakistan, and Russia. 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 as a tool for threat assessment because ideology is difficult 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 Qaeda is often offered as achieving 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 group's ideology from the outside, based on partial and limited information. For these reasons, the key for a viable assessment framework is to focus broadly across potential threats rather than on the perceived ideology of a single threat actor.

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 to define what constitutes "likely" threats and anticipated means of attack, and can shape the minimum and maximum of the threat along the developing threat "red line" (see Figure 3). 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 4. Bracketing potential hostile capacities with assumptions of likelihood facilitates narrowing planning into manageable (and often affordable and acceptable) realms. Other possible threat capabilities associated with this threat type – regardless of which threat actor processes this capability or method of attack – are then posited between these assumed limits.

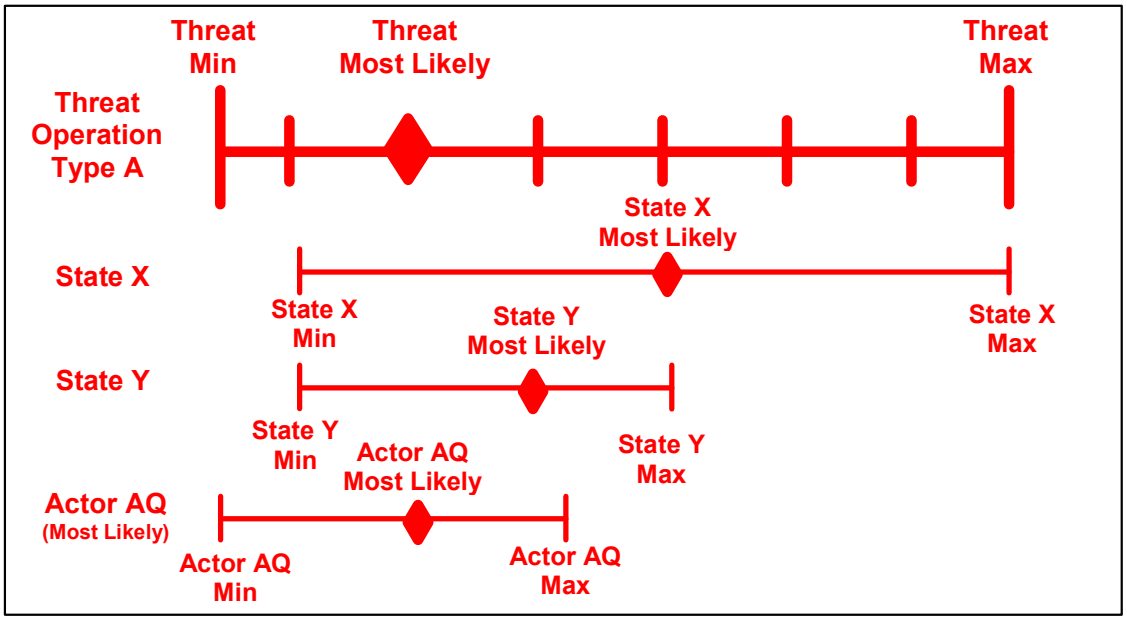

Figure 3
Developing an Assessment of Threat Capabilities

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 4. This line of operation for the threat would be built to include all unconventional asymmetric air threats aimed at the U.S. 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 as capability G7. The "transnational air attack" line of operation (if conducted with actual intelligence available), would answer questions regarding the threat while being flexible to changing conditions on threat actors, intent, and capabilities.

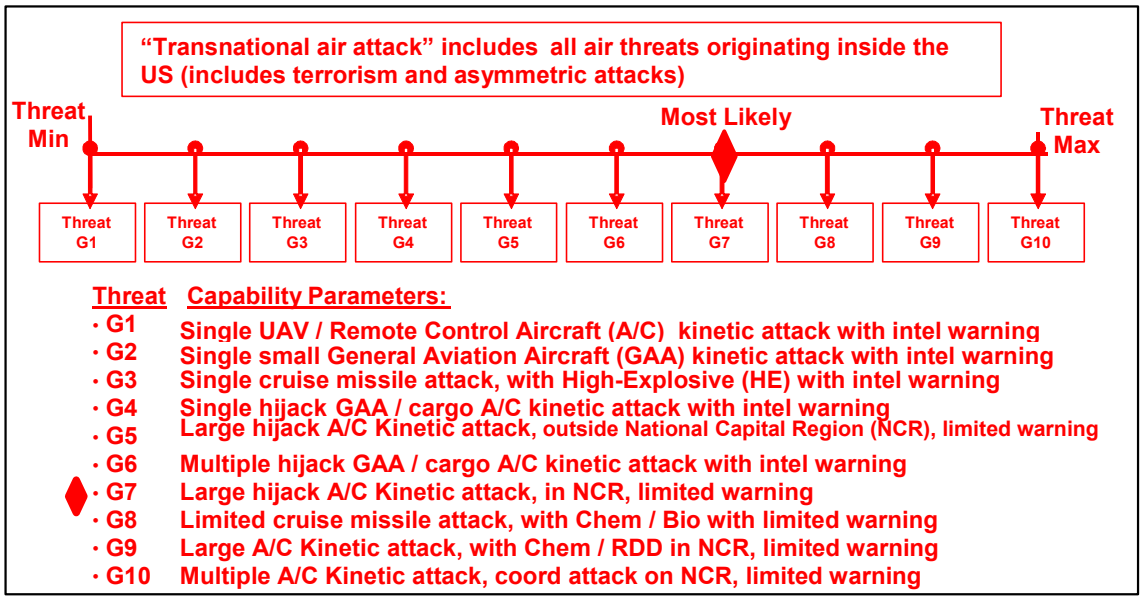

Figure 4
Example of Capabilities-Based Threat Assessments (Illustrative Purpose Only)

This capabilities-based approach to threat assessment can also work for Homeland Security-type threats where agency responsibilities overlap. An example of a simplified capabilities-based homeland security threat assessment can be seen in the transnational threat line of operation involving land attacks as depicted in Figure 5. 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 "red line" examples show enough assessment of the threat that planners can identify and develop defensive lines of operation and capabilities needed to counter these threats.

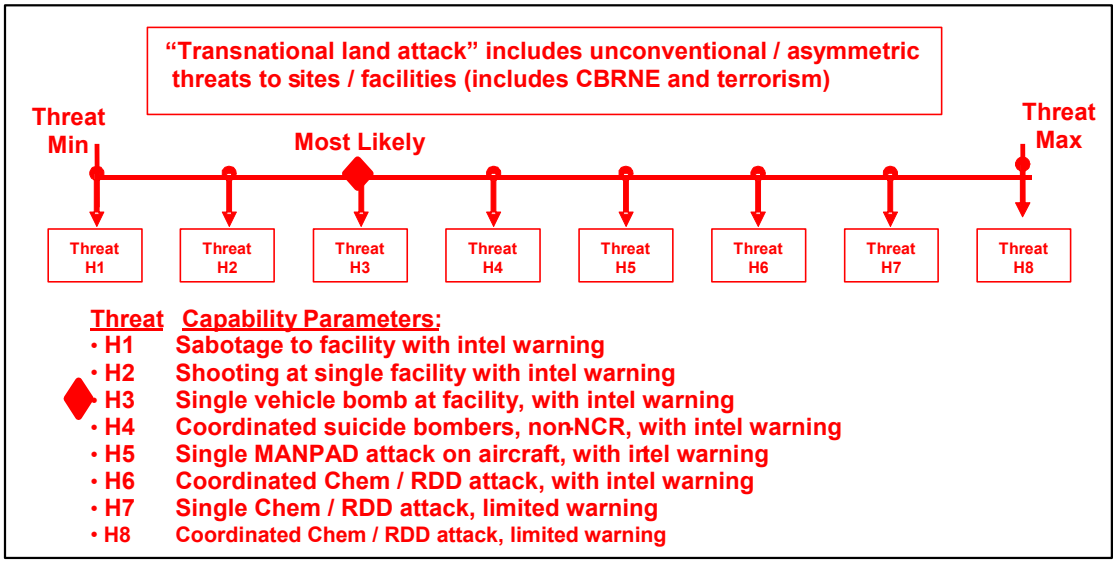

Figure 5
Example of Capabilities-Based Threat Assessments (Illustrative Purpose Only)

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 and 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 its 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. Certain "red lines" and threat capabilities can be identified as being a specific agency's responsibility because 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 U.S. Homeland. Furthermore, this process is scalable and the resulting assessments could be as complex, or as simple, as the planning needs dictate.

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 6. 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 taken in sequence concerning planning, preparation, transit, and execution, all of which can be wargamed even with a limited amount of knowledge. From this discrete and defined scenario of potential threat actions, an individual "blue" capability plan can be. The parameters of each capability data point can be expressed as planned protective and preemptive measures directed generically against the possible threat attack method.

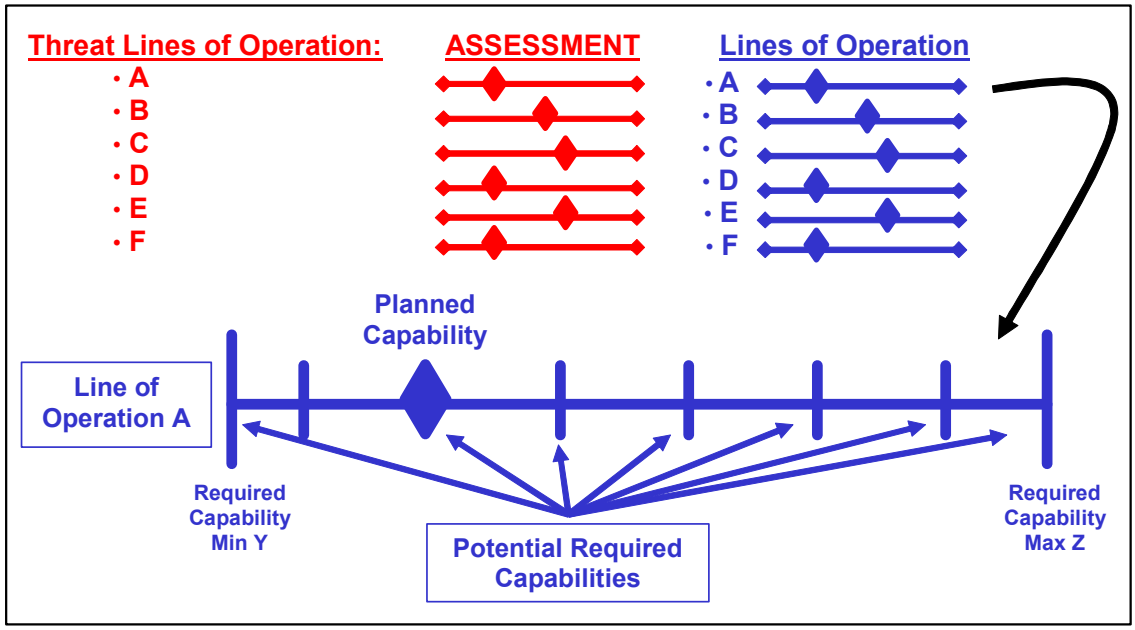

Figure 6
Capabilities-Based Planning Concept

While the intelligence assessment of threat capabilities sets 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. Decision-makers may decide either to 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 of 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.

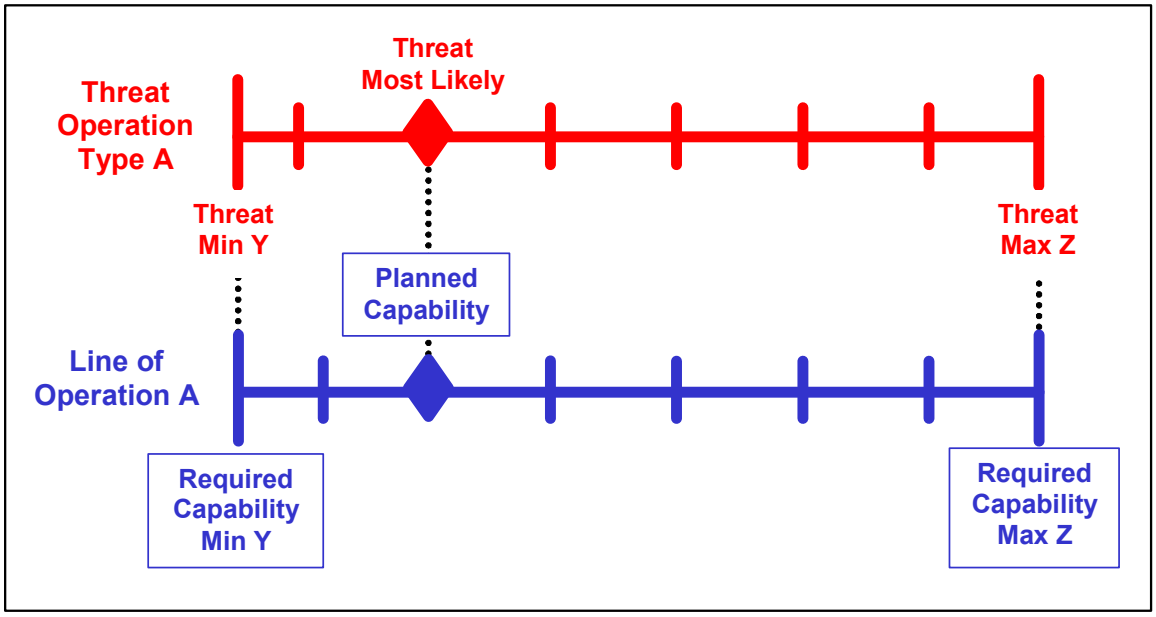

Figure 7
Countering Each Threat line of Operation

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. Planners from subordinate or outside organizations can develop independent and 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. Because capability experts are asked what they can *do* to counter a specific threat capability, detection, prevention, and defensive activities can 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"). 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.

An example of this approach is 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, homeland defense and homeland security planners can address each in turn to determine what their own organization could do to counter that individual asymmetric maritime threat aimed at the U.S. Homeland. For example, to counter the most-likely threat capability, planners would assess all possible preventative actions within their assigned area that could be used to defeat an attack by a single boat-bomb with limited warning. 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 be identified, as would the 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 discovery or suspicion of a new threat capability or the emergence of a new threat group with an innovative line of operation against the United States 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 the cyclical nature of capabilities-based planning help 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 relatively simple yet dynamic in response to 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 type and level of resources does your organization need in order to counter this specific threat?" For senior decision-makers and operators alike, this establishes a key linkage between resources and assessed threats in a straightforward manner.

Additionally, this process will reveal any required "enablers" (staff support tasks, standing or pre-designated command and control relationships, pre-approved authorities for using force, concept of employment for any alert forces, or coordinated surveillance tasks) needed 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.

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

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 number 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 number of dedicated resources can be stated as counter to that level of risk, as well as less robust threat capabilities (i.e., a preventative capability for multiple truck bomb attacks could claim to address the threat of a single truck or car bomb). However, planners may recommend, and decision-makers may select, either to assume a greater degree of risk by moving the "Planned Capability" threshold to the left (only addressing lower magnitude threat capabilities) or to increase the resource commitments to "buy down" the risks of less-likely, but greater-magnitude threat capabilities (see Figure 8).

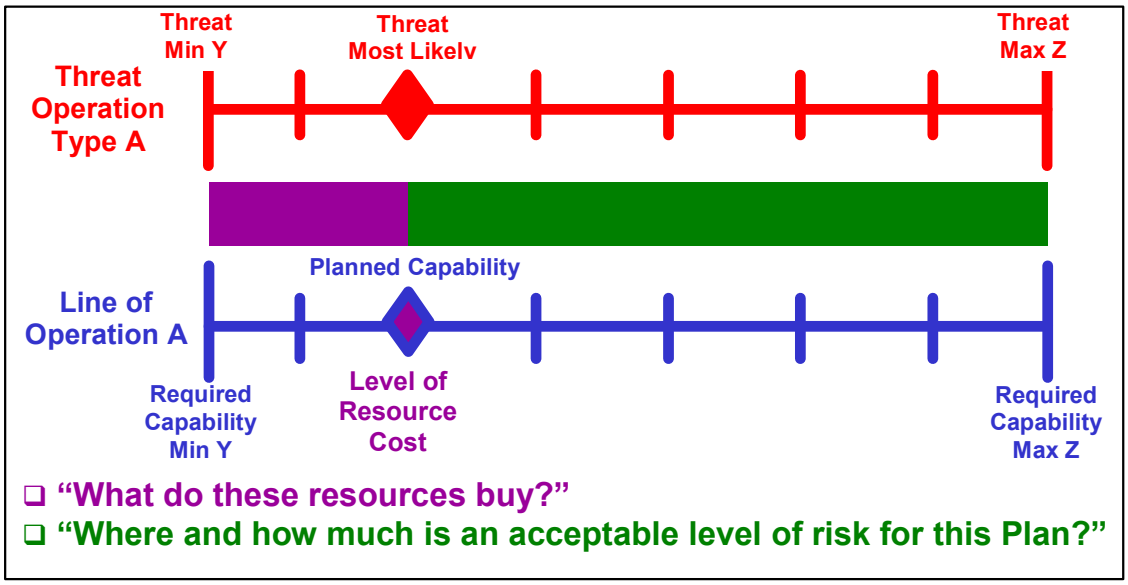

Figure 8
Assessing Resource Levels and Risks

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 homeland defense and homeland security planning, now this decision is better facilitated and the risk-versus-resources trade-offs are better understood.

This approach also can be used to identify and mitigate mismatches in capabilities. As depicted in Figure 9, this is conceptually as basic as comparing likely threat capabilities and

available prevention capabilities. Where no counter capabilities exist, mitigating long-term risks requires investment and research strategies to develop what is necessary. 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 a 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 salient point of the analysis portrayed in Figure 9 is that this approach allows for a method of both developing and expressing these mismatches to senior decision-makers.

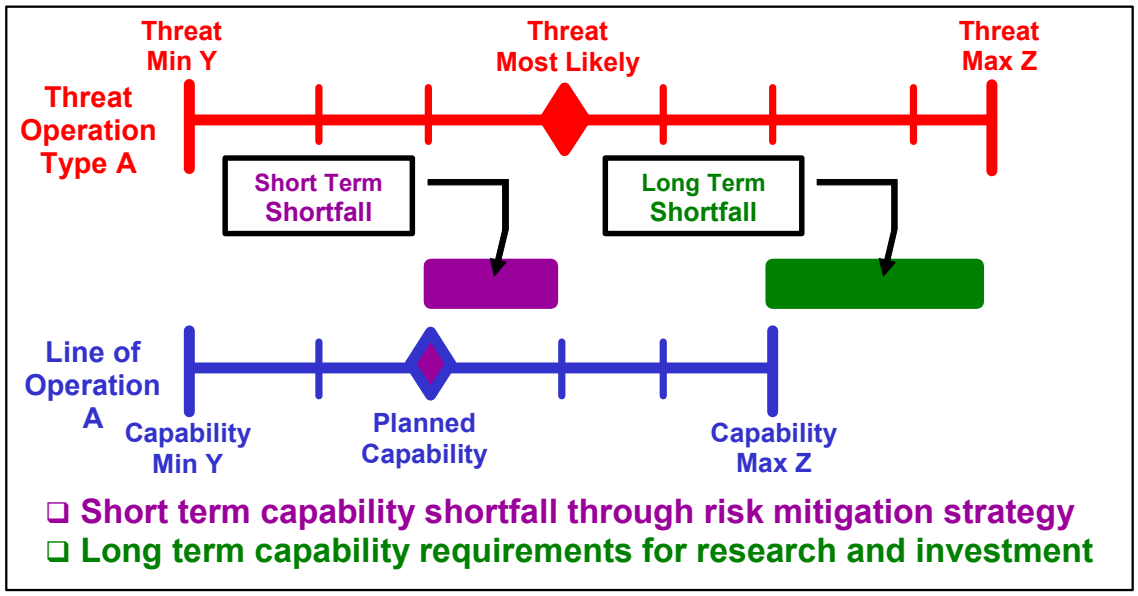

Figure 9
Determining Capabilities-Based Shortfalls

This capabilities-based approach to planning introduces both flexibility and adaptability by helping planners to define a menu of required capabilities 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 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. But modified and tailored capabilities packages could also provide a general deterrence value by demonstrating an ability to counter threat lines of operations. The end result is a comprehensive "menu" of options to prevent and defeat attacks, expressed as a list of potential lines of operation against the threat and a list of specific capabilities required to meet and overcome inherent challenges in homeland defense and security planning.

CONCLUSION: The Adaptability of a Capabilities-Based Contingency Methodology

As required by the defensive mission of protecting the United States, capabilities-based threat assessment allows a greater focus on the "how" and not the "who" of the threat. Planners need to identify the threat of a truck bomb, for example; it matters little to defense and security planners

which group actually recruited the driver or 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 homeland defense or homeland security planners a defined and detailed threat to plan against. This alone would be welcome in nearly all contingency discussions on protecting the U.S. against terrorist threats as a method to overcome challenges of uncertainty haunting current homeland defense and security planning efforts.

One of the fundamental advantages of the capabilities-based planning process is that it is explicit. In expressing the threat assessment and resulting capabilities menu, the planning process model is rendered transparent. Assumptions and choices are tested and challenged in order to constantly revise, update, and improve the contingency plan. The planning process should integrate the needs and experience of senior decision-makers by presenting plans in a comprehensible format and allowing iterative involvement at every level of management and across different agencies and organizations. 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 exceeds the overall objective to overcome uncertainty with flexibility in planning.

Capabilities-based planning can therefore be seen as a way to combine the strengths of the threat-based and scenario-based planning methods while maintaining the required level of flexibility given the evolving nature of the threat. Because of the diffuse threat environment and the great probability of the enemy's use of surprise, each piece of new intelligence further refines what threat capabilities exist. Any "actionable intelligence" triggers the execution of pre-planned defense and security capabilities with required resources already identified and enabled. Secretary of Defense Donald 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 neighborhood and keep bad guys off the streets. And you know that a big German Shepherd doesn't hurt, either.[16]

While all this may seem like 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 a burglar or terrorists. 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.

---

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

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

[3] 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." 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, D.C.: US Government Printing Office, 2000), I-4.

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

[5] Ibid., vi.

[6] Ibid., iii.

[7] *NSHLS*, 2.

[8] These four challenges for threat-based planning are 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.

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

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

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

[12] 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.

[13] This "building block" approach is addressed as a key element in capabilities-based planning in Davis, *Analytic Architecture for Capabilities-Based Planning*, 4.

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

[15] Ibid., 60.

[16] Rumsfeld, "Transforming the Military"