Applying Risk-based Decision-making Methods/Tools to U.S. Navy Antiterrorism Capabilities

Mr. Charles Mitchell
ABSG Consulting Inc.
Alexandria, VA
(703) 519-6387
cmitchell@absconsulting.com

Commander Chris Decker
U.S. Navy
OPNAV Ashore Readiness
(703) 601-1634
chris.decker@navy.mil

INTRODUCTION

Prior to the attack on the *USS Cole* and the events of September 11, 2001 (9/11), the U.S. Navy (Navy) was developing antiterrorism (AT) programs to address potential terrorist attacks in a resource-constrained environment. Amidst unprecedented tragedy associated with these and other terrorist strikes against U.S interests, both domestic and abroad, government agencies, the armed forces, and private companies have rapidly executed a vast array of security improvements to ensure mission capability and protect personnel, critical facilities, transportation systems, and other infrastructure. The Navy has allocated resources to local commanders to mitigate these identified force protection challenges; however, development of Navy-wide investment strategies based on assessment of threat or vulnerabilities proved programmatically elusive, thus creating the need for a different investment protocol.

The AT efforts within the armed forces initially focused on identifying all potential threats and vulnerabilities. While funding was installation-centric, resource constraints limited the extent to which these broad-based, wholesale changes could be made to all Navy installations. During this time, the Government Accounting Office (GAO) in its report, *Combating Terrorism: Actions Needed to Improve DoD Antiterrorism Program Implementation and Management* (Ref. 1), recommended that the Department of Defense (DoD) establish a management framework for allocating resources to AT efforts. In a subsequent report, *Combating Terrorism: Actions Needed to Guide Services' Antiterrorism Efforts at Installations,* (Ref. 2), GAO noted that a comprehensive risk management process could be an effective foundation for allocating antiterrorism resources.

With the Navy's establishment of the Commander, Navy Installations (CNI), Navy-wide program and execution alignment were set into place to leverage programs and outcomes across all Navy installations worldwide. In addition, CNI intended on achieving a risk-rationalized investment strategy while achieving improved programmatic and execution efficiencies. Accordingly, CNI began establishing a management framework for allocating resources to a risk-rationalized AT investment strategy.

Given the challenges of allocating limited resources among many AT capabilities, each with demonstrated abilities to reduce the vulnerability of individuals and property to terrorist acts, the Navy is incorporating risk-based decision-making (RBDM) processes (i.e., decision processes that are repeatable, consistent, and defendable) into its resource allocation model. As with most decisions for preventing future losses, analysts cannot judge the decisions simply by whether or not a loss occurs. This is especially apparent when dealing with terrorist risks where there is limited historical experience to assist in making risk estimates.

This paper describes how the Navy is implementing traditional RBDM methods/tools to support resource allocation decisions, including the following:

- Prioritizing gaps in AT capabilities according to security risk
- Determining which AT capabilities to fund in upcoming years, based on security risk impact compared to cost
- Optimizing limited investment capital for AT needs

This paper emphasizes how traditional RBDM methods/tools are proving effective in the security risk management field. These examples may serve as a model for other organizations wrestling with many of the same issues.

RISK BASICS

Risk is a multifaceted issue and must be addressed with methods that are appropriate for the decisions being made. Historically, risk assessment and risk management professionals have focused on accident risks, natural hazard risks, business interruption risks, project risks, and financial risks. In these areas, organizations have used very systematic processes and tools to understand and prioritize these diverse risks (especially those with catastrophic consequences) so that limited resources can be effectively applied to reduce risk. Figure 1 characterizes the foundational elements for developing an understanding of risks so that they can be effectively managed.

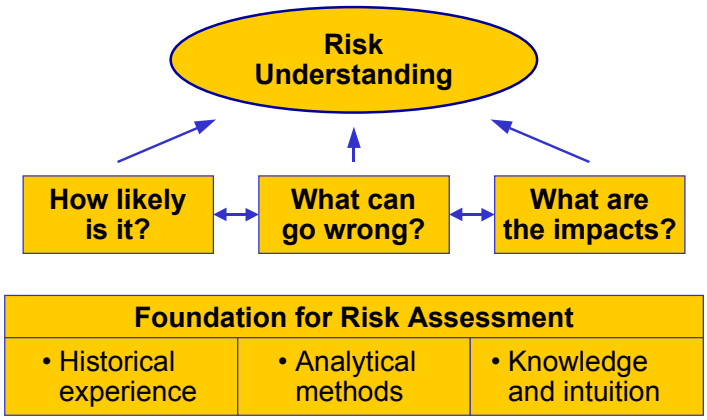

Figure 1 Foundational Elements for Developing an Understanding of Risk

In recent years, security risk (another broad category of risk with potentially catastrophic consequences) is receiving significant attention. And, while security risks require a different approach than other types of risk, the same fundamentals apply. Terrorist attacks and sabotage events are a different type of threat posing risks in much the same way as other threats.

APPLYING RISK MANAGEMENT CONCEPTS TO SECURITY

Traditionally, risk has been measured as:

Risk = Frequency (F) x Consequence (C)

where

Frequency (F) = Initiating Event Frequency x Probability All Safeguards Fail

In some Operational Risk Management (ORM) applications, risk is measured as:

Risk = Severity (S) x Probability (P) x Exposure (E).

In this case Probability (P) and Exposure (E) define the frequency component.

In security risk management, the frequency element is separated into two parts as follows:

Risk = [Threat (T) x Vulnerability (V)] x Consequence (C)

where

- *Threat* is a measure of the likelihood that a specific type of attack will be initiated against a specific target (i.e., a scenario)
- *Vulnerability* is a measure of the likelihood that various safeguards against a scenario will fail
- *Consequence* is the magnitude of the negative effects if the attack is successful. Some organizations, including the Navy, use the term criticality to describe the impact of an event.

Security risk can therefore be collapsed into the fundamental risk attributes of frequency (or probability) and consequence, and thus be measured in essentially the same way as other risks, but with slightly different terminology. Of course, just as with other types of risk, simply understanding and measuring risk are not enough. Effective risk management systems that implement and sustain important risk controls are needed to achieve tolerable levels of risk exposure (as shown in Figure 2).

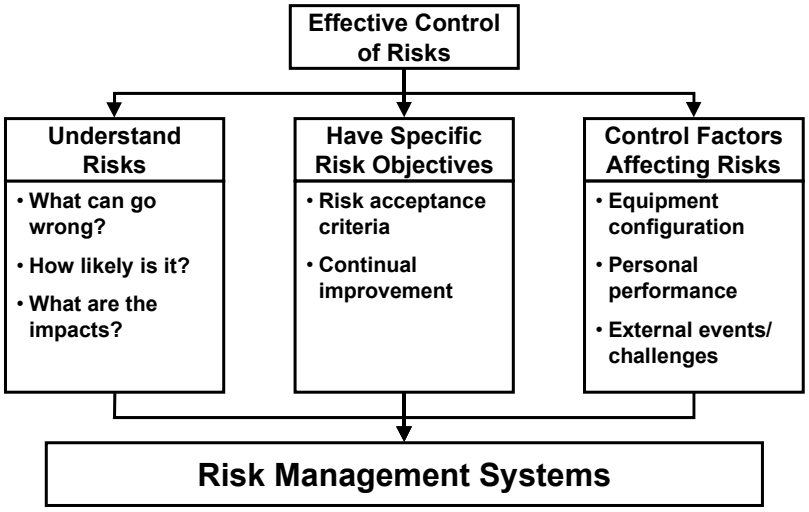

Figure 2 Key Elements of Managing Risks of Any Type

RBDM IN THE RESOURCE ALLOCATION MODEL

Figure 3 is CNI's public safety shore installation architecture for identifying AT capabilities to address the full scope of a force protection spectrum of tasks.

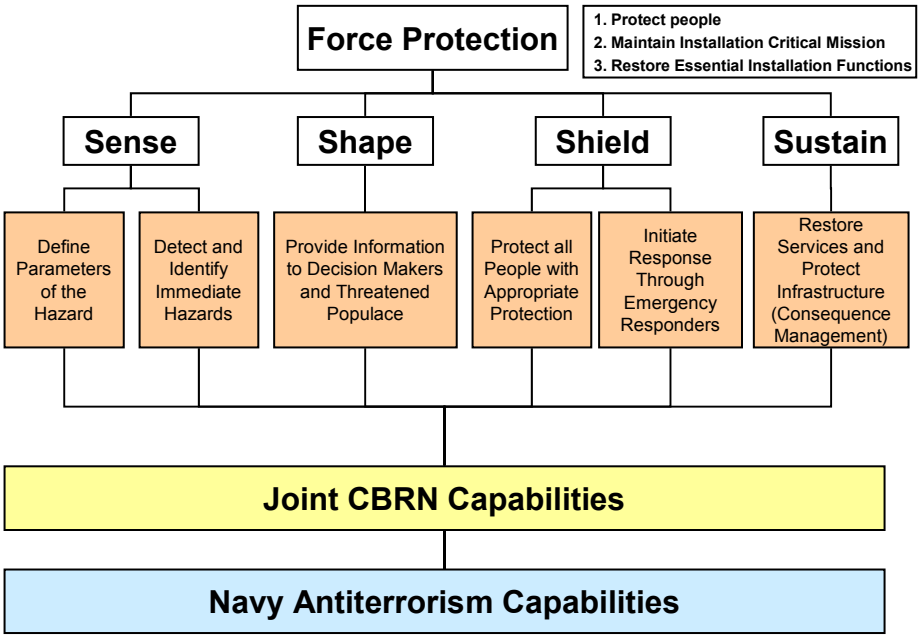

Figure 3 CNI Public Safety Architecture

The primary challenge that CNI faces in applying RBDM to the investment model is to capture risk-related information in a manner that addresses the baseline or current risk profile and the expected improvement in security risk when resources are allocated to AT capabilities. In addition, the risk reduction must be expressed in terms of a metric that can be easily compared to cost of implementation so a benefit/cost measure can be calculated.

One of the key challenges in defining a construct for collecting, organizing, and reporting the risk-based information is determining what level of precision is appropriate to support the decision being made. High or even medium precision may not necessarily be achievable, particularly when the specific technology for achieving a given AT capability is not defined or is under development. The goal is to perform the **minimum** level of analysis necessary to provide information that is at least **barely adequate** for decision making.

There are several approaches to accomplish this objective.. One means for collecting risk-based information is to define categories, then assign the appropriate threat, vulnerability, and consequence information to the appropriate category. Tables 1, 2, and 3 provide examples of threat, vulnerability, and consequence categories that can be used to capture security risk information. Assigning numerical scores to each category of threat and vulnerability and assigning "representative" loss estimates to the consequence categories provide a scoring system that will express the measure of risk in terms of loss exposure, which can be directly compared to cost of implementation; thus, providing a meaningful benefit-cost index for relative ranking.

Table 1 Threat Assessment Criteria

Category	Scenario Relative Threat Assessment Criteria
VH	This scenario is at least an order of magnitude more likely to be initiated as other "typical" scenarios (based on subject matter expert evaluation)
H	This scenario is at least twice as likely to be initiated as other "typical" scenarios (based on subject matter expert evaluation)
M	Default relative threat level for a "typical" scenario (Use this threat level unless the description for one of the relative threat levels is more fitting)
L	This scenario is at least half as likely to be initiated as other "typical" scenarios (based on subject matter expert evaluation)
VL	This scenario is at least an order of magnitude less likely to be initiated as other "typical" scenarios (based on subject matter expert evaluation)

Table 2 Vulnerability Assessment Criteria

Category	Vulnerability Assessment Criteria (including detection, security response, attack complexity, and target hardness considerations)
VH	An attack would be defeated/unsuccessful less than 10 out of 100 times (Likelihood of successful attack: >90%)
H	An attack would be defeated/unsuccessful up to 1 out of 4 times (Likelihood of successful attack: 65% to 90%)
M	An attack would be defeated/unsuccessful up to 1 out of 2 times (Likelihood of successful attack: 35% to 65%)
L	An attack would be defeated/unsuccessful up to 3 out of 4 times (Likelihood of successful attack: 10% to 35%)
VL	An attack would be defeated/unsuccessful more than 90 out of 100 times (Likelihood of successful attack: <10%)

Table 3 Consequence Assessment Criteria

Category	Death/Injury	Assets and Infrastructure	Mission Capability
VH	>1,000 deaths or serious injuries	>$1 billion	Creates critical long-term vulnerabilities in national defense
H	100 to 1,000 deaths or serious injuries	$100 million to $1 billion	Creates critical short-term vulnerabilities in national defense
M	10 to 100 deaths or serious injuries	$10 million to $100 million	Long-term disruptions in military actions
L	1 to 10 deaths or serious injuries	$1 million to $10 million	Short-term disruptions in military actions
VL	No deaths or serious injuries; relatively only minor injuries	< $1 million	No serious military/defense impact

The Navy gathered subject matter experts (SMEs) to estimate security risk for installations worldwide. These experts included representatives familiar with security threats, capability of current force protection measures, and potential consequences of attacks on installations. The SMEs performed a risk analysis that considered (1) a broad spectrum of security issues and (2) different AT capabilities as options for addressing the risks. By consensus, the SMEs selected the most appropriate category for the relative frequency, vulnerability, and consequence of the postulated scenarios and the expected reduction in each category if specific AT capabilities are applied. This "change" in risk provides a key input to the benefit-cost ratio that provides a relative ranking of the alternatives.

Cost of each capability is expressed in terms of doubling factors relative to a baseline or lowest cost capability. The initial cost categories and the assignment of AT capabilities to the categories are based on data calls for initial cost estimates for installation sustainment, restoration, and modernization. The cost categories are based on a doubling for each category. The following four categories describe the relative costs for the AT capabilities:

- Low cost
- Moderate cost = 2 * Low cost
- High cost = 4 * Low cost
- Very high cost = 8 * Low cost

Benefit-cost ranking is derived using the reduction in risk assessed by the SMEs and the relative cost ranking of each option. Figure 4 provides a relative ranking of the benefit-cost for each of the AT capabilities considered by the SMEs.

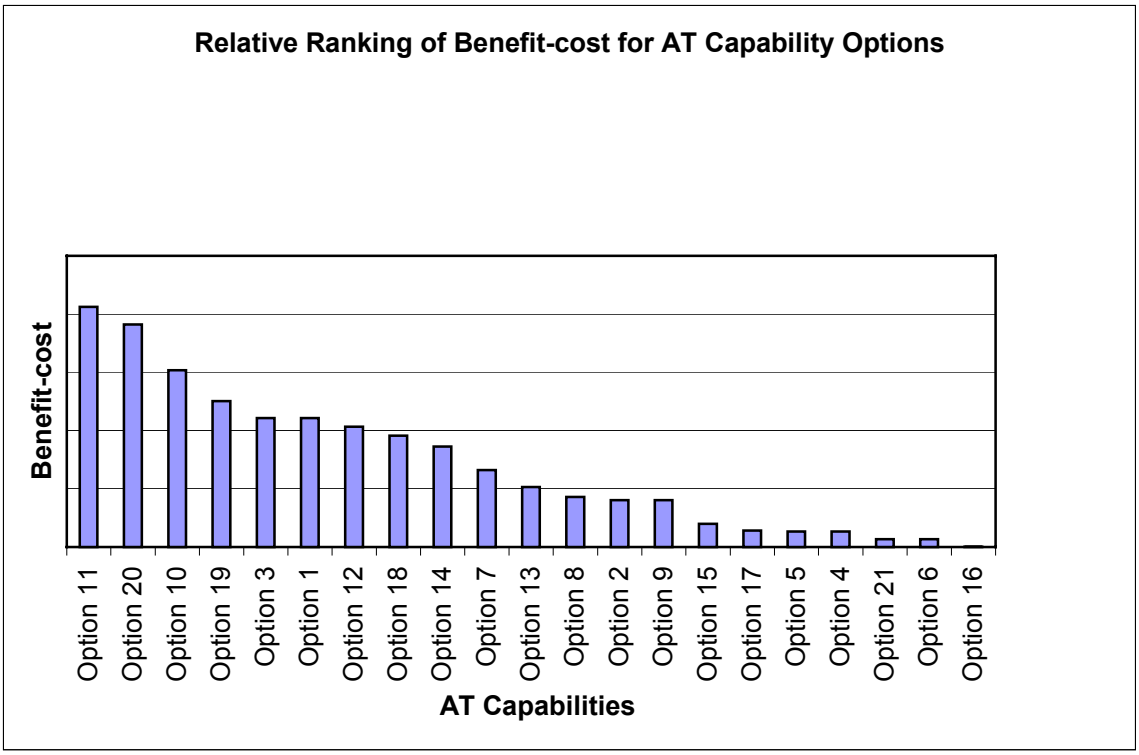

Figure 4 Relative Ranking of Benefit-cost for AT Capability Options

CONCLUDING REMARKS

Security risk management is a very visible national priority. There are many challenges ahead in understanding and prioritizing these risks as well as ensuring that limited risk mitigation resources are used wisely. Risk management tools and approaches will continue to be extremely valuable assets in the mission to ensure security.

DISCLAIMER

Opinions, conclusions, and other information expressed in this paper are those of the authors, not necessarily those of ABSG Consulting Inc. or the Navy.

REFERENCES

1. Government Accounting Office, *Combating Terrorism: Actions Needed to Improve DoD Antiterrorism Program Implementation and Management*, GAO-01-909.

2. Government Accounting Office, *Combating Terrorism: Actions Needed to Guide Services' Antiterrorism Efforts at Installations,* GAO-03-14.