

Application of Deterrence Assessment Methodologies to Commercial Ferry Attack Scenario

Dr. Newton Howard, Center for Advanced Defense Studies, newton.howard@c4ads.org

This work was supported by the U.S. Coast Guard, Department of Homeland Security

Abstract— This report proposes an approach for assessing the deterrent effect of security systems employed to prevent terrorist attacks against commercial ferries. Specifically, it analyzes the deterrent value of current U.S. MARSEC coast guard screening protocols by using a combination of deterrence assessment methodologies. Each protocol is assessed according to its effectiveness in deterring the use of a vehicle-borne improvised explosive device (VBIED) containing explosives weighing 500-1000 lbs. It is assumed that an attempt will be made to detonate this device aboard a high-capacity ferry in the US.

Two deterrence assessment methodologies are discussed: economic cost/benefit analysis and risk assessment/management. Economics literature establishes cost/benefit analysis as a valid method for utility calculation and comparison in the case of a VBIED attack. The risk assessment/management approach to deterrence assessment in this report is augmented by the methodology of Effect-Based Operations (EBO). A combination of key elements from these two similar three-step models generates a three-sided approach to assessing deterrent value of security measures. This approach can be termed the ‘triad’ approach. A mathematical formulation of this ‘triad’ provides estimates as to the cumulative deterrence effect of all security mechanisms being used in a particular protocol. Though the numbers in the ‘triad’ model are hypothetical, the model itself is useful in evaluating which combinations of security measures may lead to overall cost effective screening on ferries.

Index Terms— Deterrence assessment, marine transportation, marine vehicle control, protection, technology assessment.

I. INTRODUCTION

This report proposes an approach for assessing the deterrent effect of security systems employed to prevent terrorist attacks against commercial ferries. Specifically, it analyzes the deterrent value of screening protocols by using a combination of deterrence assessment methodologies. Each protocol is assessed according to its effectiveness in deterring the use of a vehicle-borne improvised explosive device (VBIED) containing explosives weighing 500-1000 lbs. It is

assumed that an attempt will be made to detonate this device aboard a high-capacity ferry in the US.

The threat assessment report published by ABSG Consulting Inc. for U.S. Coast Guard [1] identified the use of a VBIED as the greatest concern in commercial ferry security. Following the analysis of the ABSG, the next step is to examine existing screening protocols and their ability to deter a VBIED attack. In [2] a survey indicated that raising the required passenger, passenger vehicle, and large enclosed vehicle screening levels to meet MARSEC III requirements is cost-prohibitive to most companies. The suggestion in [3] is that current security screening protocols are incapable of providing thorough VBIED security screening while maintaining economic viability in the commercial ferry industry. Meeting MARSEC III would likely result in many ferry operators shutting down operations, thereby removing a significant source of public mass transit [4]. However, it was indicated by the same survey that if the large vehicle screening aspect of MARSEC I could be made more intensive while leaving other aspects at their normal levels, ferry companies would remain economically viable.

Prohibitive operational economics incurred at MARSEC III security performance standards come from two sources. First, the implementation of more stringent screening requires increased spending in the areas of human resources and screening equipment. Secondly, the source of economic loss at MARSEC III is caused by operation delays that come as a combined effect of increased number of screenings and longer screening times. It is critical that the security sector develops an understanding of which security measures will provide the most effective deterrence to VBIED so that these measures may be given priority. MARSEC security performance standards have been designed under the assumption that a properly executed random screening procedure at rates of 5-10% will be sufficient to produce a deterrence effect [5]. It is speculated, however, that further increases in screening percentages will be associated with a still greater deterrence effect.

This report addresses the most useful methods of assessing the deterrent effects of security measures currently practiced in the commercial ferry industry, as listed in “Scenario Selection for Ferry Special Assessment” [6]. Two deterrence assessment methodologies are discussed: economic cost/benefit analysis

and risk assessment/management. Economics literature establishes cost/benefit analysis as a valid method for utility calculation and comparison in the case of a VBIED attack. This literature is limited to direct monetary costs associated with committing and preventing hypothetical terrorist attacks. The risk assessment/management approach to deterrence assessment in this report is augmented by the methodology of Effect-Based Operations (EBO). The rationale behind this augmentation is that each methodology establishes a three-step framework for how a deterrent effect is generated [6]-[7]. A combination of key elements from these two similar three-step models generates a three-sided approach to assessing deterrent value of security measures. This approach can be termed the 'triad' approach. A mathematical formulation of this 'triad' provides estimates as to the cumulative deterrence effect of all security mechanisms being used in a particular protocol. Though the numbers in the 'triad' model are hypothetical, the model itself is useful in evaluating which combinations of security measures may lead to overall cost effective screening on ferries.

II. SCOPE

The primary scope of this report is concerned with the estimation of the deterrence effect of existing security countermeasures and protocols (specifically screening) against a terrorist attack scenario. The report addresses a possible attack on a high-capacity passenger ferry (500+ passengers), committed using a VBIED. Analysis of previous VBIED attacks suggests that such an attack would most likely be carried out using a large truck or van [8]. While the primary and secondary effects of different size VBIEDs are still being modeled, it has been established that a device weighing close to 1000 pounds would most likely deliver catastrophic damage and loss of life if detonated aboard any of the high-capacity ferries. The report's scope will assume that the target ferry and port have been under surveillance by possible terrorists, providing them with detailed information about the security measures at the site.

Within this scope, 'deterrence effect' will be viewed as: "the degree to which security measures affect the planning, preparation, calculation and perception of a particular attack by the potential attacker." More specifically, deterrence assessment strategies will be applied to the specific screening measures that are undertaken by large-scale ferry operators. These measures will be examined first in terms of each individual security measure and second in combination of these security measures within protocols. Particular attention will be given to the protocols, security measures, and the prescribed screening levels required by the MARSEC Directive 104-5.

Certain additional assumptions concerning scope are embedded in the task that this report is designed to address. Throughout the report, the attacker will be assumed to be determined, and therefore not whimsically deterred; rational, and therefore susceptible to rational models for the decision-making process; and incapable of resorting to an alternative method when deterred from a VBIED attack.

III. DETERRENCE MEASUREMENT AND ASSESSMENT METHODOLOGIES

A. Definitions and overall approach

In order to identify applicable deterrence assessment methodologies it is necessary to compose a working definition of deterrence and establish an understanding of this phenomenon's composition. This section will provide that definition and present it in a conceptual model. As a necessary component of the definition of deterrence, the concept of a 'deterrent' will also be defined. Next, a literature review will discuss applicable deterrence assessment methodologies. The literature review introduces assessment frameworks specific to other academic disciplines. These frameworks can be adapted to assessing the deterrence effect of security measures such as the protecting force. They are applied from the areas of risk assessment/management (enabled by Effects-Based Operations approach) and economic cost/benefit theory.

1) Existing deterrence definitions:

The following is an examination of several area-specific definitions of deterrence. The pertinent information from these definitions will be synthesized in order to create a working definition specific to this paper. Consequently, an expanded definition of 'deterrence assessment' is stated.

Military Science

According to military scientists, the definition of strategic deterrence is: "The prevention of adversary aggression or coercion that threatens vital interests of the United States and/or our national survival. Strategic deterrence convinces adversaries not to take grievous courses of action by means of decisive influence over their decision making." A closely related U.S. Department of Defense definition [9] is: "[t]he prevention from action by fear of the consequences. Deterrence is a state of mind brought about by the existence of a credible threat of unacceptable counteraction." These particular frameworks focus on deterrence as a strategy of prevention of courses of action. In these definitions it is the responsibility of the protector to change an adversary's strategic decision making.

Transportation Security

The U.S. Department of Transportation takes a slightly different view of deterrence. In the *Motor Carrier Management and Threat Assessment Study* [10] deterrence is defined thusly: "Countermeasures which are visible to potential attackers and which deter an attack by raising the risk of apprehension or lowering the probability of success." Fear is referenced specifically as a deterring factor. Therefore, deterrence can be viewed as part of a cognitive process. The goal of this type of deterrence is to change the attacker's mind frame, thereby dissuading the attack.

Working Definitions

Each of the above definitions carries an important quality of deterrence. The military science definition expresses strategy in that there is a need to assess the adversaries' calculations of risks, rewards, costs and benefits. The transportation security

definition references cognition, specifically apprehension, in deterring attacks. It is appropriate to combine these ideas to create a more comprehensive working definition of deterrence that includes influence on the adversary's perception.

In the following paragraphs, *deterrence* shall be defined as: "a cognitive event in the mind of an adversary considering an attack that occurs—through influence by strategic behavior, planning and action—when the adversary perceives that even the attempt of an attack will result in his objectives not being met." This definition of deterrence is meant to address the 'cognitive moment' when an attack is halted. In turn, 'assessment' expresses the success of deterrence as a quantitative measure. Therefore, an appropriate definition of 'deterrence assessment' would be: "the evaluation of feasible techniques of deterrence expressed as a quantitative measure within defined thresholds."

For the purposes of this task, it is necessary to properly qualify what could be considered as a 'deterrent' in the mind of an attacker. The concept of *deterrent* is derived from the above definition of deterrence. Since deterrence is something that can only occur in the mind of an adversary, that moment can never fully be known by anyone except for that adversary. However, the deterrence moment but it can be approached. While it is not possible to comprehensively know when deterrence as a cognitive event happens, it is possible to determine if some protections are 'deterrents' or: "measures that are known both to an adversary protector and are determined to have discouraged an adversary from attempting an attack to some degree." In this sense, a 'deterrent' is separate from the event of 'deterrence' because it is a quantifiable element that is not known solely by the adversary. In turn, it is possible to assign value to different deterrent elements. This concept is especially important in the consideration of deterrence assessment. While deterrence, as it occurs in the mind, is not possible to qualify, deterrents can be assigned value and be seen as contributing to deterrence.

Working model of deterrence effect

In light of the above definition of deterrence, it is necessary to demonstrate that concept as a composite of multiple factors—cognitive and otherwise—that can occur pre-attack, under attack or after an attack. The proposed model will combine aspects from the Department of Transportation Security Countermeasures [11] with considerations from working definitions. The DOT Security Countermeasures propose three phases of potential attacks: (1) Pre-attack (2), During attack, and (3) Post-attack. Embedded in these three phases are several countermeasures, e.g., Preparedness, Detection, and Mitigation, that operate according to a sequential timeline. One such countermeasure is deterrence. While the DOT sequential list of countermeasures are important for both attacker and defender to consider, deterrence cannot be properly expressed as a potential countermeasure.

Accordingly, a comprehensive framework of deterrence should consider explicitly reinforcing components that operate within physical countermeasures (i.e. preparedness, detection, and mitigation) and cognitive states. The DOT model does not

explain the relations of the items on the list by drawing connections between its components or referencing cognition, those factors determined to be essential to the concept of deterrence. Thus, an alternate, more comprehensive model is necessary.

The proposed deterrence effect model (figure 1), like the DOT example, takes into account three main aspects of a potential terrorist attack¹ (pre-attack, during attack, post attack) and potential countermeasures. In contrast to the DOT table, the influence model takes these aspects and countermeasures to a more complex dimension. The proposed model views deterrence as the compound of visual or otherwise observable countermeasures. The deterrence effect model illustrates deterrence as part of decision-making calculus.² This model splits the three-aspect step of the DOT example into two distinct parts: (1) preparation for an attack and (2) physical occurrence of attack. The model, depicted in Fig. 1, considers all aspects of an attack (pre-attack, under attack, and post attack countermeasures) as influencing the attacker.

The model demonstrates that all security measures, not just the pre-attack ones, may be taken into consideration for deterrence. Let's take the response measures as an example. Suppose ferry A experiences a terrorist attack, and emergency response time at site A is better than on site B. If mass casualties are the goal of the attacker, then site A is not as attractive as B. Increasing the level of responsiveness at site B (assuming the attacker is aware of the change) may shift this balance the other way³. Therefore, effectiveness of during- and post-attack deterrence countermeasures is a factor in considerations deterrence strategies, and all elements in section (2) relate back to the cognitive event of deterrence.

B. Deterrence measurement and assessment methodologies

Deterrence, as defined in this study, is the effect that knowledge of, assumptions about, and subjective perception of

¹ The consideration must be made that the proposed reasoning is attack or scenario based. While logical reasoning is applied on attacks, it is not enough. Attacks may be not homogenous, or linear (i.e. you can't deduce one from the other by induction or abduction reasoning using one logical operator). Attacks are in fact inhomogeneous, heterogenous. Arguably expected effect or anticipated effects of attacks are most likely homogenous or linear if conducted by the same group. This leads to the idea of terrorist signatures.

² In the context of this paper we are considering deterrence as a binary (e.g. an attack is deterred and does not occur or an attack is not deterred and does occur). The cognitive processes expressed above are more complex than the illustrations and/or explanations provided. Because of the length and complexity of the full explanations of each cognitive process in full, they are perhaps better left to a more in depth explanation in another paper. The force of deterrence is constantly in play against the plan of a potential attacker. It is possible that an adversary may consider several avenues of attack and be dissuaded at different cognitive or physical points on the diagram.

³ An important effect of deterrence that is in the realm of cost/benefit analysis is that of substitution. A deterrence method that is effective at countering a particular type of attack will increase the likelihood of other modes of terrorists' activity, and this feedback mechanism should be included in the assessment. Substitution possibilities among terrorist tactics arise when alternative modes of operations produce the same basic commodities (e.g., political instability, media attention) in varying amounts. Substitution is enhanced when attack modes possess closely related outcomes and are logistically similar. This idea is also important because the potential benefits from implementing a deterrence procedure (e.g., decrease in casualties) must be adjusted for substitution into other life-threatening terrorist actions.

implemented security measures have on the decision-making process of a potential attacker. As deterrence affects the attacker's decision-making process *before* the attack, it is hard to quantitatively *measure* this effect directly. The closest approximation would probably be interviews with captured terrorists or criminals, which would allow analysis of information about planned attacks that were not executed for various reasons. It is beyond the scope of this report to consider such a source of information.

As opposed to the evaluation of interview data, this report focuses on models that decompose the phenomenon of deterrence into a set of factors. The effects of these factors can be evaluated separately, and can prompt actions on the side of the security force. The analysis is guided by what the Strategic Deterrence Joint Operating Concept [12] defines as the attacker's *decision calculus*. The SD JOC model defines the "ways" and "means" by which the "end" of strategic deterrence is achieved through decisive influence over adversary decision-making. An adversary's strategic deterrence decision calculus contains three primary elements:

- Adversary perception of the benefits of a course of action
- Adversary perception of the costs of a course of action
- Adversary perception of the consequences of restraint (i.e., what will happen to them if they do not take the course of action)

The above concepts illustrate an attempt by the security force to understand the potential benefits of an adversary's attack against potential costs. Consequently, the "ways" listed below are the tools for implementing effective strategic deterrence, which can be applied to terrorism deterrence. These "ways" are closely linked in practice and often overlap in their application. The "ways" include:

- Denying Benefits
- Imposing Costs
- Inducing Adversary Restraint

The working definition of deterrence and Figure 1 establish deterrence as a cognitive process. In order for deterrence to be effective, it must be able to assess how an action will affect the decision-making process of an attacker. Two general methodologies that can describe such effects are cost/benefit analysis and risk management. The former deals with increasing or decreasing the cost or benefit for an attacker. The latter studies risk as the primary restraints on operation. While both methodologies can be used for describing the processes in the physical world, it is important to keep in mind that the categories of cost, benefit, and risk are highly *perceptual* in nature. Accordingly, this allows for their use in assessing effects of deterrence on cognitive processes.

1) *Economic cost/benefit analysis*

The body of literature in economic theory presents a method of deterrence assessment in hostage taking. Atkinson, Sandler and Tschirhart [13] use economic models to test empirical bargaining-theory hypotheses in terrorist hostage taking scenarios. Cauley [14] uses economic theory to evaluate antiterrorist deterrence measures and postulate the effect of

those methods within an economic framework. Yetman [15] seeks to expand upon the guidance that these approaches propose by focusing on the economic analysis of screening for terrorists. In this analysis Yetman uses an economic approach—specifically *costliness*—to point out the weaknesses in screening as a deterrence method.

The aforementioned literature lacks an effective method for assessing the monetary costs and benefits as considered by terrorists. Economic postulations that terrorist activity will respond to market forces do exist. However, there is not yet an effective way to calculate the external incentives available to an attacker [16]. Similarly, the methods used to calculate the costs of carrying out a complex terrorist attack are confounded by the presence of innumerable variables. For this reason, existing cost/benefit models tend to focus on the general behavior trends associated with deterrence activities. Those models are unspecific as to which aspects of a particular attack are considered costly or beneficial [17]. In addition [Sandler04] postulates that the costs and benefits of specific deterrence policies are insufficiently analyzed.

2) *Risk Management/Assessment Approach*

Risk management/assessment provides an indirect methodology for deterrence assessment. Although often considered unconventional actors, terrorists are organized in their attacks and objectives. Like any other organization that carries out goal-based tasks, terrorists must on some level consider the possibility that their task may fail. Therefore, perpetrators of terrorist attacks are forced to evaluate the risks that they may face. As a recent RAND study states:

...[a]lthough causing a member of al Qaeda to change his stripes may be out of the question, deterring individuals from attacking individual targets is not. To the contrary, the empirical record shows that even hardened terrorists dislike operational risks and may be deterred by uncertainty and risk. A foot soldier may willingly give his life in a suicide mission, and organizations may be quite willing to sacrifice such pawns, but mission success is very important and leaders are in some ways risk-averse. [18]

Following this reasoning, it is practical to view deterrence assessment in terrorist attack scenarios from a practical risk assessment/management viewpoint. Therefore, it becomes necessary to review literature concerning risk assessment/management approaches.

Shrader-Fredchette [19] and McKim [20] agree that risk assessment is the obvious precursor to risk management. According to Shrader-Fredchette, the process can be viewed as a "flow" of procedures: (1) *identification* of hazard, (2) *estimation* of harm, (3) *evaluation* of danger relative to other harms, and (4) *policy development* in which risk management is done. Once risk assessment has been completed it is possible to move to management of calculable risk. McKim posits a Risk Management Cycle (RMC), which includes the following:

1. *Risk Identification*: Risks are pinpointed and assessed. From this evaluation, it is decided which risks will be managed. Many unnecessary factors will

be eliminated at this phase (such as low probabilities of occurrence. External risks—those which are outside the scope of the problem but nevertheless affect the risk—should be identified.

2. *Risk Analysis*: Most advanced stage of RMC. Defined as a list of risks combined with an assessment of the probabilities and impacts of each risk. An important aspect of this phase is information dissemination. If the analysis is not presented in workable and understandable format and distributed to the proper officials, the effort can be wasted.
3. *Risk Response*: Uses the information gleaned from the previous two phases to develop a plan of action. The main idea is to eliminate as much risk as possible: often operations that are “too risk averse” will fail.
 - a. *Risk Reduction*: Using tools such as scheduling (moving the time or date of an activity), education (informing those who are taking part in the activity of the inherent risks and how to deal with them), and even redesign (modify a plan to reduce the risks) can help drastically reduce risk and militate success.
 - b. *Risk Allocation*: “Risk allocation refers to the party or parties that will accept a portion or all of the responsibility for the consequences of the risk.” Transferring different risks amongst involved parties can also provide a useful method of managing risk. Allocating risk to parties with the most control, the least investment in a project, or those who are best equipped to handle risk can be beneficial. [21]

The central thrust of Sharder-Fredchette’s analysis is that perceived and actual risks do not exist as discrete and insular concepts. In fact, the consequences of accepting such an idea would lead to “undesirable consequences.” Moreover, it is often the case that whether or not a risk is defined as perceived or actual, it can be dealt with in the same manner [22]. In this evaluation there are numerous reasons why one should avoid maintaining separate categories for perception and actual risk.

C. The Triad Model of Deterrence Assessment

A deterrence assessment methodology must be capable of determining how effectively a security measure influences the decision of an attacker. Using a combination of the Risk Management Cycle (RMC) and Effects Based Operations (EBO), it is possible to effectively illustrate the steps that allow a security measure to result in a deterrent effect.

The first step is to understand the attacker’s decision-making process with respect to risk assessment. The RMC outlines how a security measure in the physical world is translated into a deterrence effect within the mind of an attacker. This process consists of three steps: risk observation, risk perception, and risk response. Risk observation, is the point at which an attacker becomes *mentally* aware of an aspect of the *physical* world. Once aware of a security

measure, the attacker advances to the risk analysis step, where he assesses the degree to which a security measure endangers his mission objective(s). In this step, a security measure must elicit an interpretation of increased risk if it is to generate a deterrence effect in the response phase. Once the final step of risk response is reached, the security measure’s window to deter attack has expired. If after observing and analyzing the measure, the attacker responds by advancing with his attack, then the measure has failed to generate a deterrence effect.

If RMC translates physical measures into cognitive deterrence effects, a security force can rely on the principle of Effects-Based Operations to determine which security measures will most likely generate a deterrence effect. The protector uses EBO in order to influence the course of action that the adversary may take by affecting his thoughts and actions in a way in accordance to the interests of the protector [23]. Effects-Based Deterrence (EBD), as a subset of EBO, acknowledges the same three steps as the RMC—observation, perception, and behavioral effect [24] — and provides three criteria for choosing effective security measures. The first criterion is based on the RMC risk observation step (observation in EBD terminology). The criterion of perceived observation requires that a security measure is apparent enough that attacker will become aware of it. Once an attacker becomes aware of the measure, it enters the attacker’s RMC where it can, in turn, affect his behavior. The second criterion, which we will refer to as perceived accuracy, relates to the RMC analysis step (perception in EBD). A measure, once observed, must be relevant to the mode of attack that is to be deterred. For example, a biological attack sensor would not be relevant to an attack using only explosives. The third criterion, perceived reliability, also works in the risk analysis of the RMC. This criterion describes the expected probability that an observed threat will be active at the time of attack.

Within the model of risk assessment, affecting the attacker’s RMC is the only way that a security measure can generate a deterrence effect. Together, the three criteria describe the three ways in which a security measure can affect the risk observation and risk analysis phases of the attacker’s RMC. Such an analysis is, in effect, a qualitative deterrence assessment methodology.

Through a review of materials provided by HSI and a general literature review of cost/benefit analysis, risk assessment/management, and EBO, it is evident that these methods can be applied as deterrence assessment methodologies. Because none of methodologies is effective in isolation, this paper proposes a model that combines elements of EBO and risk management approaches. With some alterations, the three qualitative deterrence assessment criteria described above can be incorporated into a quantitative model for estimating the deterrence effect of a given security measure. The mathematical model that is rooted in the RMC and EBD will be labeled the Triad model.

Modeling the Triad Conceptually

The ‘Triad’ model, depicted in Fig. 2, is based on a three variable equation intended for qualification of each protection method as a deterrent. Each variable of the equation is

intended to correspond to a cognitive state in the mind of an adversary that would contribute to deterrence. The qualities shall be defined as:

- α = Perceived observable quality of protection measure
- β = Perceived accuracy of protection measure
- γ = Perceived reliability of protection measure

In order to use these variables (α), (β) and (γ) to conduct an overall quantitative comparison among different protection measures, a value ranging from 0.0 to 1.0 must be assigned to each variable. Zero (0) = lowest value possible value that could correspond to a cognitive state. In the case of (α), a zero would represent a complete absence of perceived observation of protection measure by an adversary. One (1.0) = highest possible assigned value that could correspond to a cognitive state. In the case of (α), a one would represent the highest perceived observation of protection measure by an adversary. In order to determine the overall deterrent effect (Δ) of each protection measure, the variables must be multiplied: $\Delta = (\alpha)(\beta)(\gamma)$. Because the purpose of this equation is to evaluate a cognitive state and it is not possible to fully understand the mind of an adversary, it is impossible to assume that the value of any one variable is zero (0.0) or one (1.0) can be assigned to any state. However, it is possible for the value of a variable in this equation—outside the scope of this paper—to *approach zero or one*.

IV. IMPACT OF SECURITY MEASURES ON DETERRENCE

Modeling the Triad Mathematically

Through analysis of MARSEC [25] screening levels eight separate deterrent protection components can be discerned. For simplicity, each deterrent is assigned a variable:

1. 100% vehicle screening = x_1
2. Less than 100% vehicle screening = x_2
3. Canine Sweep = x_3
4. Physical inspection with Canine = x_4
5. Light manual inspection (metal detector, cursory visual inspection) = x_5
6. Heavy manual inspection (inside the car, open the hood/trunk inspection) = x_6
7. X-Ray machine = x_7
8. Explosive detector = x_8

Thus each Screening protocol is represented by P_j where j = protocol level as follows:

$$P_1 \equiv x_1 \vee x_2 \Rightarrow x_3 \Rightarrow x_4$$

$$P_2 \equiv x_1 \vee x_2 \Rightarrow x_5 \Rightarrow x_6$$

$$P_3 \equiv x_1 \vee x_2 \Rightarrow x_7 \Rightarrow x_4$$

$$P_4 \equiv x_1 \vee x_2 \Rightarrow x_8 \Rightarrow x_6$$

For each variable x_i where $i = 1, 2, \dots, 8$ three values are assigned: $\alpha(x_i), \beta(x_i), \gamma(x_i)$. These values are strictly between 0 and 1 correspond to:

- α = Perceived observable quality of protection measure
- β = Perceived accuracy of protection measure
- γ = Perceived reliability of protection measure

Let $\Delta(x_i) = \alpha(x_i)\beta(x_i)\gamma(x_i)$ is the value of the deterrent representing x_i . The objective is to compare and contrast the deterrent values of the screening protocols.

Hypothetical Example 1: single deterrent

To more effectively illustrate the Triad approach, a hypothetical example will be presented in which values will be assigned to $\alpha(x_i), \beta(x_i), \gamma(x_i)$.

For the Canine Sweep = x_3

1. $\alpha = 0.7$, i.e. Perceived observable quality of protection measure is high.

Explanation: Assume that the attacker has been observing cars and trucks entering a ferry and has noticed several of them are checked by canine sweep.

2. $\beta = 0.8$ Perceived accuracy of protection measure is high.

Explanation: Assume that the attacker perceives accuracy of the canine sweep is difficult to defeat.

3. $\gamma = 0.3$ Perceived reliability of protection measure is low. Explanation: The attacker knows that there are few canine teams or that canines must rest often.

The result:

$$\alpha(x_i) = 0.7$$

$$\beta(x_i) = 0.8$$

$$\gamma(x_i) = 0.3$$

$$\Delta(x_3) = 0.168$$

In this hypothetical example, two values— $\alpha(x_i) = 0.7$ and $\beta(x_i) = 0.8$ —were high, yet the single occurrence of a low value ($\gamma(x_i) = 0.3$) brought the overall deterrent value of the canine sweep to 0.168. This illustrates that *all* perceived aspects of the security measure must have high values for the deterrent to have a high value overall.

Hypothetical Example 2: deterrent protocols

As explained in example 1, subjective analysis of each deterrent attribute of a security measure, $\alpha(x_i), \beta(x_i), \gamma(x_i)$, allows us to assign values to each. x_3 (canine sweep) as a deterrent is highly observable and highly accurate. However it may not be reliable as dogs may require food and rest. Using the same subjective analysis the other security measures were assigned values (see Chart 1 below).

Chart 1: Deterrent variables

| | α | β | γ | Δ |
|-----------|----------|---------|----------|----------|
| x1 | 0.99 | 0.99 | 0.99 | 0.97 |
| x2 | 0.5 | 0.5 | 0.5 | 0.13 |
| x3 | 0.7 | 0.8 | 0.3 | 0.17 |
| x4 | 0.8 | 0.85 | 0.5 | 0.34 |
| x5 | 0.6 | 0.3 | 0.4 | 0.07 |
| x6 | 0.8 | 0.7 | 0.8 | 0.45 |
| x7 | 0.9 | 0.7 | 0.8 | 0.50 |
| x8 | 0.9 | 0.4 | 0.8 | 0.29 |

Once all measures are assigned deterrent values, the overall deterrent effect of the protocols can be calculated. For each security protocol, there are three levels of screening [HSI04c]. From the diagram in [HSI04c] it is logical to assume that deterrence values are meant to increase as the screening levels increase. In order to remain consistent with this hypothesis, it is necessary to compute movement from each security level as an increase in deterrence. Since the first level of all four screening protocols contains the same security measures (i.e. $x_1 \vee x_2$) the increase in the value of the deterrent from screening level one to screening level two is omitted. Therefore the applicable increase should occur between screening level two and screening level three. A mathematical representation of that increase calculates the ratio between $\Delta(x_i)$ level 2 and $\Delta(x_i)$ level 3. If the ratio is greater than 1 then the deterrent value is increasing. If the ratio is less than 1 then the deterrent value is decreasing. A protocol consistent with the HSI model and its mathematical equivalent must contain increasing relative deterrent values. (see Chart 2)

Chart 2: Protocol ratios

| | $\Delta(L 2)$ | $\Delta(L 3)$ | $\Delta(L 3)/\Delta(L 2)$ |
|-----------|---------------|---------------|---------------------------|
| P1 | 0.17 | 0.34 | 2.02 |
| P2 | 0.07 | 0.45 | 6.22 |
| P3 | 0.50 | 0.34 | 0.67 |
| P4 | 0.29 | 0.45 | 1.56 |

Example 3: constructing a high deterrence screening protocol using the Triad

The aforementioned inferences made, it is possible to construct a highly deterrent screening protocol from the hypothetical numbers in examples 1 and 2. The proposed protocol would look like this:

$$P \equiv x_1 \vee x_2 \Rightarrow x_6 \Rightarrow x_7$$

x_1 = 100% vehicle screening

x_2 = Less than 100% vehicle screening

x_6 = Heavy manual inspection (inside the car, open the hood/trunk inspection)

x_7 = X-Ray machine

The rationale behind this selection is as follows: Level 1: Every screening protocol begins with $x_1 \vee x_2$ so level 1 in this protocol begins the same way; Level 2 and Level 3: the highest two deltas in table 1 correspond with x_6 (.45) and x_7 (.5). Since increased deterrent value is desirable the order is from level 2 to 3 is x_6 then x_7 . Because the security measures in x_6 and x_7 may present a high cost, it may become necessary to create alternate, cost effective protocols with high deterrence values. Using the data from examples one and two those protocols would look like:

$$P \equiv x_1 \vee x_2 \Rightarrow x_3 \Rightarrow x_4$$

$$P \equiv x_1 \vee x_2 \Rightarrow x_4 \Rightarrow x_6$$

What can be inferred from the hypothetical examples? Although the above situations use hypothetical numbers as deterrent values, the logical pattern that emerges from the synthesis of these situations creates a valid deterrence assessment methodology. Example one presents a subjective way to assign values to each protection measure as a deterrent and illustrates that that *all* perceived aspects of the protection measure must have high values for the deterrent effect to be high. Example two provides an effective way to assess the increasing deterrence within each protocol. Example three proposes a method for constructing the highest valued deterrent protocol from examples one and two. If the non-arbitrary numbers for each variable within a security measure are all high, that measure can be considered an effective deterrent. Accordingly, if a method can be devised of assigning non-arbitrary values to each security measure, the mathematical formula outlined in example two can be applied to effectively assess deterrence for a particular protocol. By using the rationale in example three, a highly deterrent protocol can be constructed.

V. CONCLUSION

This report specifies several contributions to deterrence assessment. Foremost, working definitions of deterrence, deterrent and deterrence assessment are formulated. Deterrence is recognized as part of a cognitive process. The "deterrence effect model" illustrates part of what the cognitive model of deterrence might look like in the mind and alludes to those aspects of the physical that may contribute to that cognitive process. The purpose of this paper, however, is not simply to outline a cognitive model for deterrence. Rather, this report is intended to outline applicable methodologies for deterrence assessment, such as cost benefit analysis and risk management assessment. The report is also intended to indirectly assess the value of deterrence through already established frameworks.

Furthermore, the introduction of a ferry attack scenario provides specific security measures and screening procedures as action items that require a specific value for their deterrent effect. The proposed approach combines risk assessment with

effects-based operation strategy to introduce a model that is able to value each specific security measure as a separate deterrent that contributes to the cognitive process of deterrence. As values are assigned to security measures, it becomes possible to arrange those measures an order that will maximize deterrent value.

The triad model has obvious limitations. It is lacking a scale for the value of each of its variables and/or security measures. For this reason, values must be hypothetically posited. Interestingly, cost/benefit analysis could be considered as a methodology for assigning value to the aforementioned unvalued variables of the triad. The integration of cost benefit analysis into the assignment of value for variables in the triad would effectively incorporate risk management, EBO and cost benefit analysis into one comprehensive methodology for deterrence assessment.

APPENDIX?

ACKNOWLEDGMENT

Dr. Howard thanks Sergey Kanareykin, Daniel Simon, Kurt Eifling and David Simon for their significant contributions to this report.

WORKS CITED

- [1] Scenario Selection for Ferry Special Assessment, Deliverable 2. Received from HSI by direct communication, October 2004.
- [2] *Ferry System Security Screening Status: Consolidated Report June 2004*. Received from HSI by direct communication, October 2004.
- [3] *Ferry System Security Screening Status: Consolidated Report June 2004*. Received from HSI by direct communication, October 2004.
- [4] Homeland Security Institute. 2004-b. *Synopsis of High-Capacity Ferry Survey*. Received from HSI by direct communication, October 2004.
- [5] Homeland Security Institute. 2004-b. *Synopsis of High-Capacity Ferry Survey*. Received from HSI by direct communication, October 2004.
- [6] Scenario Selection for Ferry Special Assessment, Deliverable 2. Received from HSI by direct communication, October 2004.
- [7] Edward A. Smith, *Effects-Based Deterrence (Chap 16)*, from *Globalization and Maritime Power, National Defense* University, http://www.ndu.edu/inss/books/Books_2002/Globalization_and_Maritime_Power_Dec_02/17_ch16.htm
- [8] Jobbagy, M., Literature Survey on Effects-Based Operations: A Ph.D. study on measuring military effects and effectiveness, Netherlands Laboratory for Applied Scientific Research, 2003.
- [9] Scenario Selection for Ferry Special Assessment, Deliverable 2. Received from HSI by direct communication, October 2004.
- [10] US Department of Defense, *Strategic Deterrence Joint Operating Concept*, February 2004.
- [11] U.S. Department of Transportation Research and Special Programs Administration, *District of Columbia Motor Carrier Management and Threat Assessment Study*, prepared by Volpe National Transportation Systems Center Research and Special Programs Administration, U.S. Department of Transportation, October 2003 <http://ddot.dc.gov/ddot/lib/ddot/clayimages/motorcarriermanagement/security.pdf>
- [12] US Department of Defense, *Strategic Deterrence Joint Operating Concept*, February 2004.
- [13] Atkinson, S.E., Sandler, T. and Tschirhart, J. (1987) "Terrorism in a Bargaining Framework", *Journal of Law and Economics*, 30 (1), 1-21
- [14] Cauley, J. and Inn, E.I. (1988) "Intervention Policy Analysis of Skyjackings and Other Terrorist Incidents. *American Economic Review*, 78(2), 27-31
- [15] Yetman, James. "Suicidal Terrorism and Discriminatory Screening: An Efficiency-Equity Trade-off." School of Economics and Finance, University of Hong Kong, April 16th, 2003.
- [16] Frey, B. and Luechinger, S. 2002. *Working Paper No. 136 Terrorism: Deterrence May Backfire. Working Paper Series*. Institute for Empirical Research in Economics, University of Zurich.
- [17] Frey, B. and Luechinger, S. 2002. *Working Paper No. 136 Terrorism: Deterrence May Backfire. Working Paper Series*. Institute for Empirical Research in Economics, University of Zurich.
- [18] Sandler, T. and Enders, W. 2004. "An Economic Perspective on Transnational Terrorism." *European Journal of Political Economy*. 20(2), pp. 301-316.
- [19] Paul K. Davis, Brian M. Jenkins, *Deterrence and Influence in Counterterrorism: A Component on the War on al Qaeda*, RAND, 2002
- [20] Shrader-Fredchette, K.S., *Risk and Rationality, Chapter 6: Perceived Risk and Expert-Judgment Strategy: The Case for a Negotiated Account of Risk and Rationality*, University of California Press: Berkeley, 1991
- [21] McKim, Robert A., *Risk Management: Back to Basics*, Cost Engineering. 34 no. 12 (December 1992): 7-12.
- [22] McKim, Robert A., *Risk Management: Back to Basics*, Cost Engineering. 34 no. 12 (December 1992): 7-12.
- [23] Shrader-Fredchette, K.S., *Risk and Rationality, Chapter 6: Perceived Risk and Expert-Judgment Strategy: The Case for a Negotiated Account of Risk and Rationality*, University of California Press: Berkeley, 1991
- [24] Edward A. Smith, *Effects-Based Deterrence (Chap 16)*, from *Globalization and Maritime Power, National Defense* University, http://www.ndu.edu/inss/books/Books_2002/Globalization_and_Maritime_Power_Dec_02/17_ch16.htm
- [25] Edward A. Smith, *Effects-Based Deterrence (Chap 16)*, from *Globalization and Maritime Power, National Defense* University, http://www.ndu.edu/inss/books/Books_2002/Globalization_and_Maritime_Power_Dec_02/17_ch16.htm
- [26] Screening Protocols matrix. Received from HSI by direct communication, October 2004.

REFERENCE

- Berejikian, Jeffrey D., *A Cognitive Theory of Deterrence*, Journal of Peace Research, Vol. 39-2, 2002. (<http://jpr.sagepub.com/cgi/reprint/39/2/165>)
- Blomberg, S., Hess, G., and Weerapana, A. 2003. *An Economic Model of Terrorism*.
- Franz Dietrich, *Terrorism prevention: a general model*, <http://www.uni-konstanz.de/ppm/Dietrich/Papers/FDietrich-PreventTerrorism.pdf>
- Ender, Walter and Sandler, Todd. *An Economic Perspective on Transnational Terrorism*, European Journal of Political Economy, June 2004
- Frey, B. and Luechinger, S. 2003. *Working Paper No. 171: Measuring Terrorism*. Working Paper Series. Institute for Empirical Research in Economics, University of Zurich.
- Jacobson, S. and Kobza, J. 2002. *Assessing the Effect of Deterrence on Aviation Checked Baggage Screening Strategies*.
- Konrad, K. (2004). *The Investment Problem in Terrorism*. *Economica*. Number 71, 449–459.
- Lakdawalla, D. and Zanjani, G. 2002. *Working Paper: Insurance, Self-Protection, and the Economics of Terrorism*. RAND Institute for Civil Justice.
- Lapan, H. E., & Sandler, T., *To bargain or not to bargain: That is the question*. American Economic Review, 78(2), 16-20.
- Lapan, H.E. and Sandler, T. (1988) "The Calculus of Dissent: An Analysis of Terrorists Choice of Targets." *Sythsese*. 76, 245-261.
- Maritime Transportation Security Act (MTSA) of 2002
- Rowe, William D., *An Anatomy of Risk*, John Wiley & Sons, 1977
- Rübbelke, D. 2004. *Differing Motivations for Terrorism*. Department of Economics, Chemnitz University of Technology. Chemnitz, Germany.
- Sandler, T. 2003. *Collective Action and Transnational Terrorism*. The World Economy. Volume 26, Issue 6. p 779.
- Sandler, T. and Acre, Daniel M, *Terrorism and Game Theory*, Simulation & Gaming, Vol. 34 (3) September 2003.

US Coast Guard. 2004. Maritime Security (MARSEC) 104-5; Passenger Vessel/Ferry Performance Standards. Received from HSI by direct communication, October 2004.

Dr. Newton Howard holds a Doctoral degree in Cognitive Informatics from La Sorbonne, France. Internationally, he is a leading researcher on the Physics of Cognition (PoC) and its applications to Defense and International Security.

A graduate of the Faculty of Mathematical Sciences at the University of Oxford, his work there proposed the Theory of Intention Awareness (IA). Dr. Howard is the Founder and Director of the Institute for Mathematical Complexity and Cognition (MC2). Addressing subjects related to cognition, complexity and intentions, this institute is also active in systems engineering and international security. Dr. Howard also heads the Descartes Institute for Mathematical Methods in Behavioral Codification and Global Security, focusing on behavior models and codification to develop new approaches for counterterrorism based on in-depth analysis.

A Professor in Mathematics, Informatics and Psychiatry, Dr. Howard holds teaching positions at the Rochester Institute of Technology and The George Washington University. He is an active member of several research laboratories worldwide, including Les Écoles de Coëtquidan - École Spéciale Militaire de Saint-Cyr, and the École Militaire de Paris. Having held the posts of visiting professor/associate and defense diplomat, Dr. Howard is the director of leading international cooperation programs on Codification of Asymmetric Emerging Trends in Global Security and Information Assurance, and is a Senior Research Professor at the Cyber Security Policy Research Institute, as well as director of homeland security initiatives at [Rochester Institute of Technology](http://www.rit.edu/~hw).

Dr. Howard advises several organizations in the US special operations community and has extensive experience of working in the industry. He holds multiple US patents, and is the author of several publications in the areas of military information science, computer systems theory, and strategic thinking. He is affiliated with the US Intelligence Community and served honorably in the US Armed Forces as Strategic Intelligence Officer.