

to carry out the attack mode and any intelligence that indicated an organization was planning an attack. Lacking specific, credible intelligence that would allow an increase or reduction in the threat score for a specific attack mode, this was fixed at a constant value consistent with the Maritime Security (MARSEC) Levels previously established by the Coast Guard. The baseline assumption was that terrorist cells were operating with unknown targets and methods of attack. Changes in MARSEC Levels or specific, credible intelligence would trigger an appropriate modification in threat.

Vulnerability

The term “vulnerability” measures the conditional probability of success given that a threat scenario occurs. It evaluates the adequacy and effectiveness of safeguards (both existing and proposed).

For the N-RAT, an attack was estimated as likely to succeed only if: the target was available, the target was physically accessible to be attacked, organic security associated with the target would not detect and defeat the intended attack, and the mode of attack would be capable of producing the intended consequences by overcoming the inherent safeguards designed into the system.

If all of the above mentioned barriers fail to halt the intended attack, then the attack would result in one or more outcomes. Outcomes ranged from relatively minor to catastrophic levels. The above mentioned four elements described the targets’ overall vulnerability and were scored by the expert team.

The availability of a target measured its presence and predictability as it

relates to an enemy’s ability to plan and conduct an attack. The accessibility of a target, evaluated its physical deterrence (*i.e.*, location, perimeter fencing, *etc.*) against different attack modes. It related to physical and geographic barriers that deter the threat without organic security. Organic security of a target assessed the ability of the target’s security measures to deter the attack. It included security plans, communication capabilities, guard forces, intrusion detection systems, and ability of outside law enforcement to prevent the attack. Target hardness was a measure of the ability of a target to withstand attack. It is based on the complexity of target design and material construction characteristics.

Each vulnerability type was scored over five levels of magnitude (1–5—lowest to highest). Again, scoring benchmarks were used to help ensure consistency. Each level of magnitude in every vulnerability category was assigned a probability of allowing an attack mode to proceed. The probability for each vulnerability category was factored, along with the threat probability, in risk calculations to determine the probability term of the risk equation. The individual probabilities were then multiplied together to derive the overall probability assessment for the target/attack scenario under consideration.

Consequence

The term “consequence” is the estimation of adverse effect from the target/attack scenario and is an important consideration in risk evaluation and security planning. Six categories of effects were considered in evaluating the consequence of an attack:

death/injury, economic, environmental, national defense, symbolic effect, and secondary (follow-on) national security threat. Inherent in this consideration was the criticality of the target. For each effect category, five levels of severity were described, and scoring benchmarks are provided. Unlike vulnerability, each severity level was assigned a common consequence value for use in risk calculations. For example, the most severe economic impact consequences were considered equivalent to the most severe death/injury and symbolic effect consequences. The selected level for each factor was then converted to a representative value of potential loss for the consequence factor. These consequence scores were then summed across all appropriate categories to develop the consequence values for the target/attack scenario combination.

The estimated probability and consequence values were multiplied to calculate the overall risk for each target/attack scenario. This is essentially an estimate of the expected losses should a specific target/attack scenario occur.

Assessment Results

The following graph is a demonstration of the type of the relative-risk results the N-RAT gave. Specific results, including scores, have been designated as sensitive security information (SSI). This graph simply displays the relationship between some types/classes of vessels and facilities or port infrastructure based on their relative risk. In each line, the parenthetical (I) and (D) stands for “international” or “domestic,” respectively.

BILLING CODE 4910-15-U