Risk Management of the Maritime Terrorist Threat

Background

Since 9/11, the United States Coast Guard (USCG) has conducted an aggressive terrorist risk analysis and management program focused on direct and exploitation attacks. This program developed the Maritime Security Risk Analysis Model (MSRAM). The methodology and software tool is used to identify, characterize, and quantify risks from terrorist attacks based on the Department of Homeland Security (DHS) risk equation of Risk is a function of Threat, Vulnerability, and Consequence.

The MSRAM database contains thousands of targets and scenarios (target/attack mode pairings) across the nation's ports and waterways. This robust national dataset is the product of collaborative local level assessment efforts between USCG security experts and port stakeholders to score the risk components for each scenario. National resources including consequence modeling and security studies, intelligence data, and reliability engineering techniques support their analysis. As part of a formal revalidation cycle, MSRAM risk is updated annually. Risk analysts can also update MSRAM risk scores as conditions change in the operational environment or when new information becomes available. Beyond assessing and analyzing risk, MSRAM provides risk management capabilities to evaluate risk mitigation strategies at the tactical, operational and strategic levels. MSRAM risk information informs resource allocation decisions at every level, including the DHS Port Security Grant Program, USCG Maritime Security Response Operations and regulatory development. MSRAM was awarded the USCG Innovation Award and is institutionalized in USCG policy.

The MSRAM program is currently being extended with a new framework called Maritime Security Dynamic Risk Management Model (DRMM). DRMM leverages MSRAM's quantitative risk assessment data and methods in scenario-based "what-if" simulations that project the likely impacts of maritime counter-terrorism strategies over time. It also captures estimated lifecycle costs and timetables for deploying such strategies and achieving risk reduction. By combining these outputs, DRMM enables USCG decision-makers to assess the cost-benefit (and time-benefit) tradeoffs for alternate strategies across a range of plausible future situations and identify robust security options. DRMM is being developed for the USCG by DecisionPath and ABS Consulting.

Dynamic Risk Management – Key Problems Addressed

MSRAM evaluates alternate risk reduction strategies individually, via discrete before/after "snapshots" of risk. In contrast, DRMM assesses combinations of security strategies, by projecting how they are likely to reduce risk exposure over time. DRMM also enables comparative "what-if" analyses assuming that various aspects of the security "landscape" might change in the future. In effect, DRMM provides a virtual environment for practicing alternate risk management strategies and learning from simulations rather than costly investments with unknown effectiveness.

Individual security strategies generally only address a sparse subset of attack modes and their attendant risks. For example, a single patrol boat can counter a single small boat, but cannot engage and defeat an attack involving multiple boats or a large hijacked vessel. Accordingly, DRMM supports construction and testing of portfolios of security strategies, including acquiring resources and personnel, training, and improving allocations and tactics to deploy new and existing assets.

This raises the question of how to combine risk reduction contributions from multiple independent strategies that impact a given scenario. DRMM assumes that as risk is reduced, it becomes progressively harder to achieve further gains: more effort is required to achieve the next level of improvement.

Accordingly, as DRMM projects increasing risk reduction from original levels, it progressively discounts estimates of security strategy impacts, resulting in a nonlinear model. The discounting factor can be tuned as the USCG accumulates data from quantifying risk reduction benefits of its security strategies.

Since budgets and assets are increasingly constrained, risk management decisions hinge on tradeoffs among alternate risk reduction strategies. DRMM allows analysts and decision-makers to compare the simulated values of key performance metrics to identify the relative strengths and weaknesses of alternative strategies. DRMM currently tracks and projects three strategy key performance metrics to inform strategy tradeoff analyses for decision makers:

- How much risk does a security strategy reduce over time?
- How much risk does the strategy reduce per dollar of investment over time (i.e., return on investment)?
- How soon and at what rate does a strategy reduce exposure to risk (i.e., expected time efficiency)?

Risk management strategies are developed based on specific assumptions about risk and funding, in the short and long term. As strategies are implemented over time, these situational factors continue to evolve, often outside of government control. For example, economic conditions, patterns of radicalization, and leadership of terrorist groups shift. Such changes may potentially invalidate key assumptions underlying a strategy, however reasonable they were at the initial point of decision.

In addition to the dynamic nature of the overall security environment our terrorist adversaries are adaptive. In essence, DHS agency efforts to reduce the nation's exposure to risk from terrorist attacks simultaneously increase terrorists' risk of failure. In order to achieve their goals and objectives, terrorist groups respond, typically by altering their intended targets and tactics, or developing capabilities to overcome security measures. Such "threat shifting" means that the effectiveness of risk reduction – including deterrence – is transitory, so our strategies must be adaptive in order to defeat adaptive adversaries.

DRMM addresses the first challenge by facilitating "lifecycle" decision support: as time passes, analysts periodically update scenarios based on the best available intelligence (and execution results to date). DRMM then re-projects the chosen strategy into the future. If outcomes continue to be favorable, the strategy has been re-validated. If not, DRMM acts as an "early warning system," alerting analysts promptly to emerging problems, helping them isolate variances from initial assumptions, and enabling them to define and validate suitable mid-course corrections in security strategies.

DRMM addresses the second challenge of adaptive adversaries in a similar fashion, by enabling analysts to create diverse scenarios that anticipate potential terrorist responses to proposed security strategies. For example, scenarios can incorporate assumptions as to when terrorist adversaries are likely to detect improvements in our defenses, and how (and over what duration) they are likely to modify their targeting tactics and attack capabilities. The resulting simulations provide a war gaming capability for testing and tuning strategies to ensure that they are robust against plausible terrorist adaptations before rolling them out. In effect, DRMM enables strategic planning to shift from reactive to proactive.

Finally, MSRAM enables USCG security experts to perform detailed risk analysis on individual targets (e.g., vessels, port facilities, commercial installations). However, program-level investments to reduce risk generally focus on geographic regions (i.e., clusters of targets), target types or attack modes (e.g., power plants, IEDs), or capabilities (e.g., regional communication, situational awareness, evacuation planning, etc.). DRMM rolls up its key risk reduction metrics from targets geographically from ports, Captains of the Port (COTPs), and up through the rest of the USCG command hierarchy (Sector, District, Area, Headquarters). It can also roll up risk by target type or attack mode. By aggregating risk, DRMM

bridges the gap between policy-level decisions (how and where money is spent) and MSRAM's fine-grained, physically localized target-level risk estimates.

DRMM Software Solution

DRMM employs a model-simulate-analyze software framework. The USCG has applied DRMM in pilot projects to explore alternative strategies for managing risks from small boat threats, radiological and nuclear weapons of mass destruction, and transfer threats of terrorists and materiel from foreign ports. In these evaluations, the HQ MSRAM Team considered solutions that addressed vulnerabilities and consequences as well as USCG tactical solutions to increase effectiveness and capacity of USCG boat patrol operations in a major port. These diverse risk management solutions employed one or several improved capabilities combined across the Prevent-Protect-Respond-Recover continuum. The various security solutions analyzed addressed risk reduction by mitigating vulnerabilities, accounting for Prevent and Protect. Additionally, the consequence reduction solution focused on Respond. Future analysis may look at the long term consequence reduction and infrastructure recoverability of various resiliency solutions, and can assess the cost and time efficiency of such solutions in a similar manner.

DRMM simulations projects outcomes in terms of four key performance metrics – risk reduction, total lifecycle costs, Return on Investment (ROI measured in dollars spent per unit risk reduced), and time efficiency. The ROI metric assigns credit for both reducing risk and keeping risk reduced over time (much like the effectiveness of a diet). The time efficiency metric measures the rate at which risk gets reduced over time, giving credit for solutions that reduce risk exposure earlier rather than later. These metrics enable commanders to compare alternate strategies and make critical policy-level tradeoffs relative to available resources, perceived risks, etc.

In summary, DRMM allows USCG leaders to "test drive" maritime counter-terrorism solutions across a range of alternative possible futures and identify robust security strategies. DRMM's underlying model/simulate/analyze paradigm and performance metrics are not inherently tied to maritime terrorism risks. This flexibility opens the door to applying these USCG methods and software tools to risk management problems facing other DHS agencies, such as aviation, highway, and border security, as well as to security challenges facing other critical infrastructure networks, such as systemic risks to financial markets.

DecisionPath partnered with ABS Consulting Group to develop DRMM. DecisionPath, Inc. is a supplier of custom decision support software solutions, based on our ForeTell-DSS® software platform. Other ForeTell solutions enable transformational change, support competitive drug marketing strategy, and help validate and refine performance management strategies.