Adaptive Risk-Readiness Decision Support for Infrastructure Protection

Mark F. Taylor
The MITRE Corporation
mtaylor@mitre.org

Russell J. Graves
The MITRE Corporation
digger@mitre.org

ABSTRACT

This paper presents a system concept for integrating the mass of information critical to infrastructure protection operations. Our main focus and contribution lies in (1) coupling risk assessments into a dynamic decision support process, and (2) providing a collaboration and visualization decision support interface for representing complex and changing infrastructure protection information. The system concept supports adaptive decision making based upon dynamic risk and readiness assessments. Users benefit from having a more comprehensive and up-to-date risk picture on which to base their judgments.

Keywords

Infrastructure protection, emergency management, decision support, risk assessment, resource allocation, visualization, collaboration.

INTRODUCTION

The Problem

Managers charged with protecting critical infrastructure face difficult decisions in deploying their scarce security resources so that they most effectively protect the organization's critical assets. Their decisions ideally should lead to a condition in which their limited resources are allocated against the range of known threats in such a way that: (a) overall readiness - preparedness of security operations to respond - is maximized; and (b) overall risk - taken across all protected assets - is minimized.

This paper addresses the task of achieving the conditions described in points (a) and (b) above. Important issues we focus on are:

- Threat assessments and security plans are typically static documents that are not updated dynamically to reflect changing situations.
    - How can threat assessments and security plans be made an active element in day-to-day security operations?
- Readiness - preparedness in terms of training, equipment, personnel availability, configuration of resources - is typically assessed and managed based on relatively static threat and security planning information.
    - How can operational readiness be coupled to dynamic risk assessments so that capabilities can be quickly and flexibly configured to meet changing threats?
- Scarce security resources are typically not allocated to asset protection based on up-to-date threat and risk situation information thus exposing the organization to higher risk.
    - How can limited security resources be allocated in the light of actual situational risk information so that readiness of the security organization is maximized and overall risk is minimized?

We begin by examining the complex nature of infrastructure protection in environments where: (1) multiple organizations are involved; (2) the critical assets to be protected have geographic, functional, and organizational interdependencies; and (3) the facility operations involving these assets are dynamically changing.

Example - Port of Boston

The Port of Boston presents a concrete example of this complexity. The figure below lists major infrastructure present in or adjacent to the port.

• **International Airport** • **Cruise Ship Terminal** • **Auto-Port Terminal** • **World Trade Center** • **Waste-water Treatment Facility** • **Charles River Dam** • **U. S. Coast Guard Base**	• **Container Shipping Terminal** • **Bridges (4)** • **Automobile Tunnels (3)** • **Petroleum Shipping-Storage Facilities (9)** • **Liquid Natural Gas Shipping-Storage Facilities (5)** • **Power Generating Plants (2)**

Figure 1. Port of Boston Major Infrastructure

We draw on the port example below to illustrate concepts, issues, and potential solution approaches. We selected this example because it typifies the important infrastructure problems that are our focus. Application of our approach to other settings should be clear from the explanations presented. Plans are underway to work with selected operational units at the Port of Boston to implement a proof of concept prototype system. Further discussion of these plans is contained in the final section of this paper.

Managing Complexity

The 31 facilities in Figure 1 represent only major port infrastructure - there are numerous other entities within the port. Nevertheless, these 31 facilities by themselves constitute a very complex web of interrelationships. They are run by variety of organizations including agencies of Federal, State, and Local government and a wide range of private firms and contractors. Authority and responsibility for infrastructure protection is consequently split across many entities operating at different levels. Decision making under these conditions is difficult and in emergency situations can lead to sub-optimal responses due to communication and information shortfalls.

Another factor complicating the task of infrastructure protection is the growing complexity of the facilities themselves. While many facilities are geographically compact with defined perimeters, more typical are facilities that are dispersed and without clear boundaries. In the port, for example, we have the airport, harbor, bridges, tunnels, and terminals, vessels in transit and at the dock, and ground vehicles moving into and out of the area. Further, while a smaller facility may be represented by one or a few critical assets, a more typical facility has multiple critical assets, or may be an amalgam of several facilities whose security must be managed together because of their geographic or logistical connections. Liquid Natural Gas (LNG) facilities exemplify this situation with bulk storage, pipelines, tanker vessels entering and leaving the port, vessels in process of unloading, all taking place among passenger ship traffic, waterfront hotels, restaurants, and other commercial activity. Managing LNG infrastructure protection means coordinating with the protection of nearby facilities. These facilities are at risk due to proximity to the LNG operations, and their presence close to LNG operations may in turn pose a risk to the LNG facilities.

We employ the term *readiness* to characterize the degree of preparation of an infrastructure protection operation. For dispersed facilities under multiple organization control, readiness poses special challenges. Even if one assumes availability of adequate security resources, there remains the critical issue of how security operations deploying these resources are coordinated.

Challenges

Infrastructure protection coordination and readiness in complex environments such as those just described calls for high levels of information sharing. Two specific challenges are:

1. Creating security awareness through information sharing among all organizations - Federal, State, Local, and private.
2. Supporting collaborative security decision making among organizations based upon a common view of security conditions across all facilities.

Managing Risk

A critical aspect of multi-facility security is the treatment of threat, vulnerability, and risk. Each asset can be evaluated for its vulnerabilities in relation to potential threats. From this, and an evaluation of the potential consequences of harm to the asset, an assessment of risk to the asset can be obtained. Ultimately, risk must be assessed over the range of facility assets in order to appropriately allocate and manage security resources for their protection. Having an appropriate allocation of the right resources for those facility protection situations that can reasonably be anticipated is a measure of readiness.

The port context brings out the challenge of assessing and managing risk. Traditionally, each organization performs its own risk assessments. However, this practice can lead to non-commensurate assessments. When infrastructure protection is inherently coupled, as at the port with LNG vessels and cruise vessels for example, decisions about how to allocate protection resources cannot be made accurately if the risk factors for the component assets cannot be accurately weighed one with the other.

In practice, risk and readiness are often treated in static terms. That is, risk is assessed at relatively wide time intervals, and readiness planning is handled in a similar fashion. This practice leaves facilities vulnerable because changing situations may alter the threat picture for certain assets, thus changing the risk profile across the facility's assets. Consider the relative risk to LNG facilities when a loaded tanker is at the dock to when there are no vessels docked; or the risk to a passenger vessel when it is docked full of passengers to when it has just a skeleton crew. If risk and readiness are not dynamically adjusted, then the protection configuration for the affected facilities will be misaligned to the real threats: too many guards assigned when there's no vessel and too few when a loaded vessel is present, to cite a simple example.

Moving from static to dynamic and adaptive risk management in the context of multi-organization infrastructure protection poses significant security planning and operations issues. The challenges stated below summarize their key points.

Challenges

Risk management challenges include creating an infrastructure protection capability that can

1. Dynamically adjust risk and readiness assessments.
2. Dynamically allocate protection resources according to changing assessments.
3. Support dynamic assessment and resource allocation in a multi-organization, split responsibility environment.

Approaches to Infrastructure Protection Readiness and Risk Management

MITRE has designed models for infrastructure protection where coordination and interoperation across organizations and dynamic risk-readiness planning are made the focus. These models are being deployed as prototypes and demonstrations in Regional, State, and Local settings to promote the emergence of a coherent national approach to coordinated infrastructure protection.

The following sections describe a recent design effort to provide an adaptive risk and readiness decision support environment for infrastructure protection operations in multi-organizational settings.

MANAGING RISK IN THE CONDUCT OF INFRASTRUCTURE PROTECTION OPERATIONS

Threat, vulnerability, and risk assessments are key sources for infrastructure protection planning. Risk, which combines threat and vulnerability with measures of consequence, is a crucial factor required by decision makers when choosing how to allocate limited resources to an array of potential targets. In most infrastructure situations there are several critical assets each of which should be assessed for risk. In this case, it is the overall risk across all critical assets that decision makers seek to minimize, subject to resource limitations and other constraints.

To be ultimately useful in allocating protection resources, risk assessments must be prepared based upon current threat and operational conditions. However, in many security settings, assessing risk is done relatively infrequently – not on a cycle that produces assessments reflecting actual threat conditions, which can change with events and operational factors in the facility. When assessments of risk are not closely tied to the situation on the ground there will inevitably be a tendency for risk assessments and operational protective measures to become misaligned over time. The result can be sub-optimal allocation of infrastructure protection resources; sub-optimal in the sense that overall risk has not been minimized within existing constraints.

This paper presents a model in which risk assessments are dynamically and adaptively coupled to facility operations and to security operations through a collaborative decision support system. The decision support system puts key risk assessment information in the hands of decision makers along with information on resource allocations derived from current operations. Risk assessments in this system are dynamically updated as operating conditions evolve. This allows infrastructure protection resources to be adaptively allocated according to the risks actually inherent in the situation on the ground. The system provides views and situation awareness so that real-time decisions can be made that optimally allocate limited resources thus minimizing actual risk across the facility's critical assets.

The next section describes a conceptual model for a system that achieves the effective merging of risk and operational information in a decision support environment.

AN ADAPTIVE RISK-READINESS DECISION SUPPORT MODEL FOR INFRASTRUCTURE PROTECTION

The Adaptive Risk-Readiness (ARR) model focuses on supporting decision makers from multiple organizations who are jointly responsible for protection of facilities with critical infrastructure.

The model rests on three key capabilities:

- *Sharing of information among prime players with responsibility for protection:* support for decision makers through situation awareness of current operations, including a dynamic view of protection resource allocations
- *Management of overall risk through Threat-Vulnerability-Risk (TVR) assessments:* provide decision makers with current, dynamically updated assessments across the set of key assets comprising the infrastructure
- *Use of Threat-Vulnerability-Risk assessments in combination with operational situation awareness:* support decision makers in allocating infrastructure protection resources in a near-real-time manner so as to maximize readiness and minimize overall risk to assets.

The resulting model supports *adaptive risk-readiness decision making:* the capability to adapt protection resource allocations to a dynamic view of risk across the assets to be protected. The goal is to achieve maximum readiness and minimum overall risk within operational constraints prevailing at any time. Figure 2 at the beginning of the next section illustrates these concepts.

CONCEPTS AND DESIGN PATTERNS FOR THE MODEL

The diagram below outlines the risk-adaptive decision support framework.

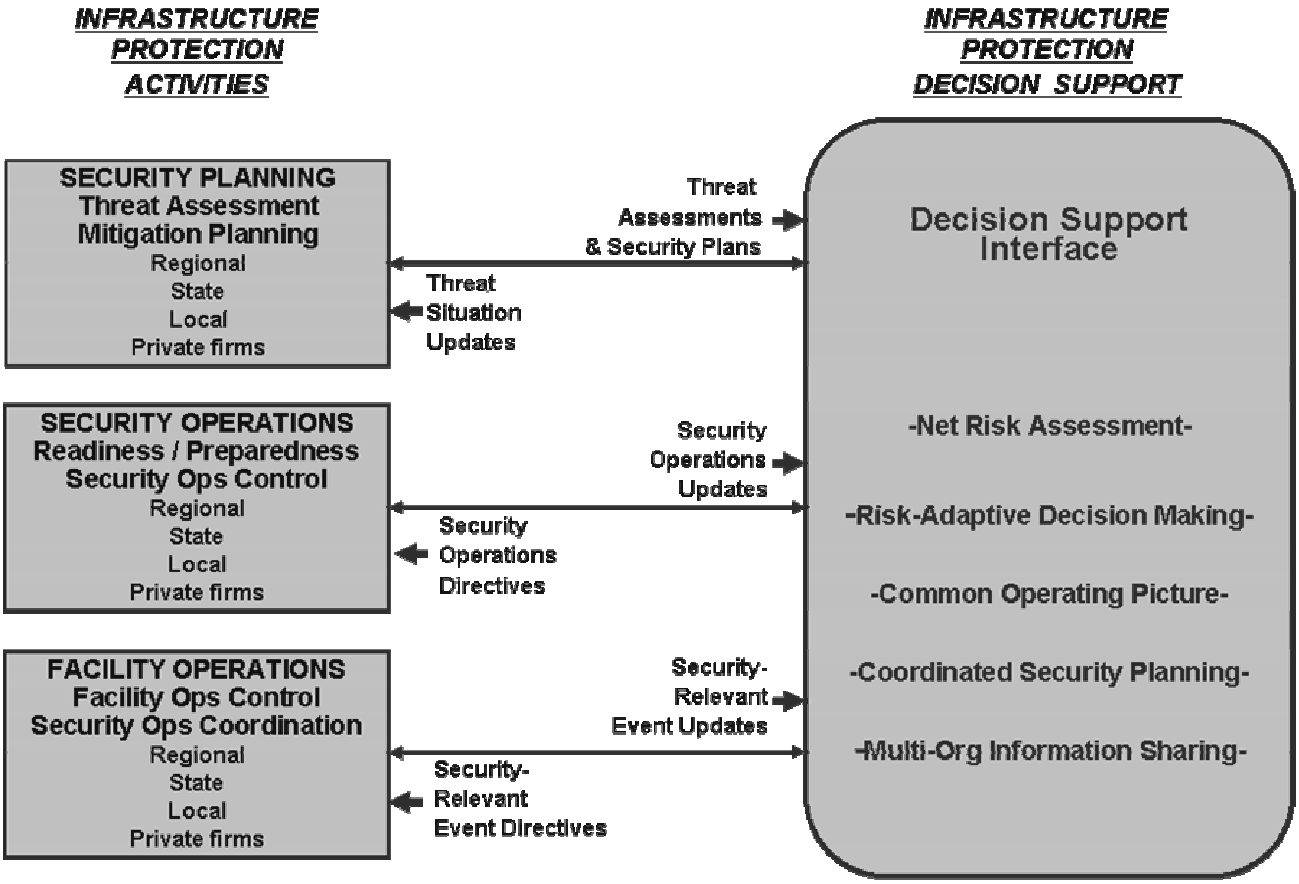

Figure 2 Adaptive Risk-Readiness Model

Figure 2 shows a notional model for the ARR system. On the left are the three principal functions that interact with the Decision Support Interface, which is shown on the right. Note that Regional, State, Local, and Private entities having a direct stake in the facility's protection are connected to the Decision Support Interface and participate in the decision making in all three functional areas. With the information interchanges shown by the arrows, the Decision Support Interface supports key collaborative decision making functions for facilities protection:

Net Risk Assessment – the ability to visualize and weigh risk viewed in consolidated fashion across the facility's assets;

Adaptive Risk-Readiness Decision Making – allowing users to adjust their security decisions based upon changing risk patterns;

Common Security Operating Picture – a visualization of the salient features of the facility's protection situation;

Coordinated Security Planning – supporting multiple players in planning based on a common security operating picture and on the risk assessments;

Multi-Organizational Information Sharing – situation awareness across the several organizations (Regional, State, Local, and Private) having a stake in the facility's security.

Operations Time Scales

The model is designed to support a range of infrastructure protection information exchanges from real-time updates coming from sensors; near-real-time information originating from operations people in the field; and regular, scheduled status updates and reports.

Organizational Scales

The model is designed to accommodate a range of organizational structures: At the small end are single-facility infrastructure complexes where the protection organizations are closely related and co-located, as in a nuclear power plant; the risk-adaptive decision support framework in this case serves as part of the facility operations center. At an intermediate scale are infrastructure complexes comprised of distributed, multiple-function facilities, as in mass transit systems, ports, airports, or electric power systems. At the largest scale are regional infrastructure consolidations where the risk-adaptive decision support serves high level officials who oversee extended groupings of infrastructures, as in regional power grids, interstate rail systems, or regional water systems.

Distributed Decision Support Architecture

The framework is designed to support multiple replicated decision support sites so that both remote and central participants can access, view, and manipulate data items. A system of privileges is used to control access and user actions.

Cross Boundary Information Sharing and Decision Support

An essential property of the model is its support for information sharing across organizational boundaries within a decision support environment. The framework does not assume any particular relationships among the organizations, leaving this to the organizations themselves to determine and enact.

What the model does supply is a common infrastructure protection picture for all players together with a collaborative decision making context within which to work together. An implication of this setup is that actual command and control authority can continue to rest with the multiple organizations who have the core responsibilities under local, state, or regional law. The framework provides a key coordination platform that supports interoperation across the several responsible organizations.

Day-to-Day Infrastructure Protection Operations and Emergency Operations

The model is designed to transition smoothly from day-to-day decision making for infrastructure protection operations to emergency operations directly preceding or following an incident.

ENABLING TECHNOLOGIES

Here, we summarize the technology base for the model outlined in the preceding section. The base includes: Network Infrastructure, Cyber Security, Collaboration, Visualization, and Risk Assessment. While each of these areas is critical to realizing the model[1], after briefly describing the first two areas we focus on Collaboration, Visualization, and Risk Assessment.

Network Infrastructure

The model is designed to support Web-based access via browsers in a Web services environment. Wireless access is also supported, including access through hand-held devices. The model is open so that new infrastructure protection applications can be connected and their data incorporated into the decision making framework.

Cyber Security

Computer infrastructure security will need to incorporate the complex set of players likely to be involved in a large facility protection operation. Considerations include exchange of information at different classification levels and use of role and privilege based access control. MITRE has research ongoing in these areas with particular emphasis on cross-boundary information exchange. However, early ARR prototypes and demonstrations, while conceptually compatible with classification and privilege requirements, will not implement them.

Collaboration and Visualization

The core of the ARR decision support environment lies in its collaboration and visualization capabilities. Current plans are to build a prototype on a commercial collaboration platform such as Groove (Groove Networks, Inc.) or InfoWorkspace (Ezenia, Inc.). The collaboration platform will provide base communication facilities in a persistent virtual workspace in which decision makers, whether co-located or not, can exchange information.

ARR's key visualization, information fusion, and common display capabilities will be supplied by a MITRE prototype, the Symbiotic Display Ensemble for Visualization and Interaction (SIDEView) [2], currently in development. SIDEView is based on the symbiotic display concept of Ragunath, et. al. [3]. As shown in Figure 3, the system provides a Knowledge Wall, a common room-sized display. SIDEView software supports interactive functions that essentially make the Knowledge Wall a *common user interface*. Users at workstations, in the room or remote, can pull a part of the display down to their own display screen and work with the same data there that created the common display on the Knowledge Wall. The system also supports workstation-to-workstation information exchange based upon the same functionality. SIDEView is being created as the base for a fluid collaborative interaction and information sharing facility, one that can support the requirements of ARR.

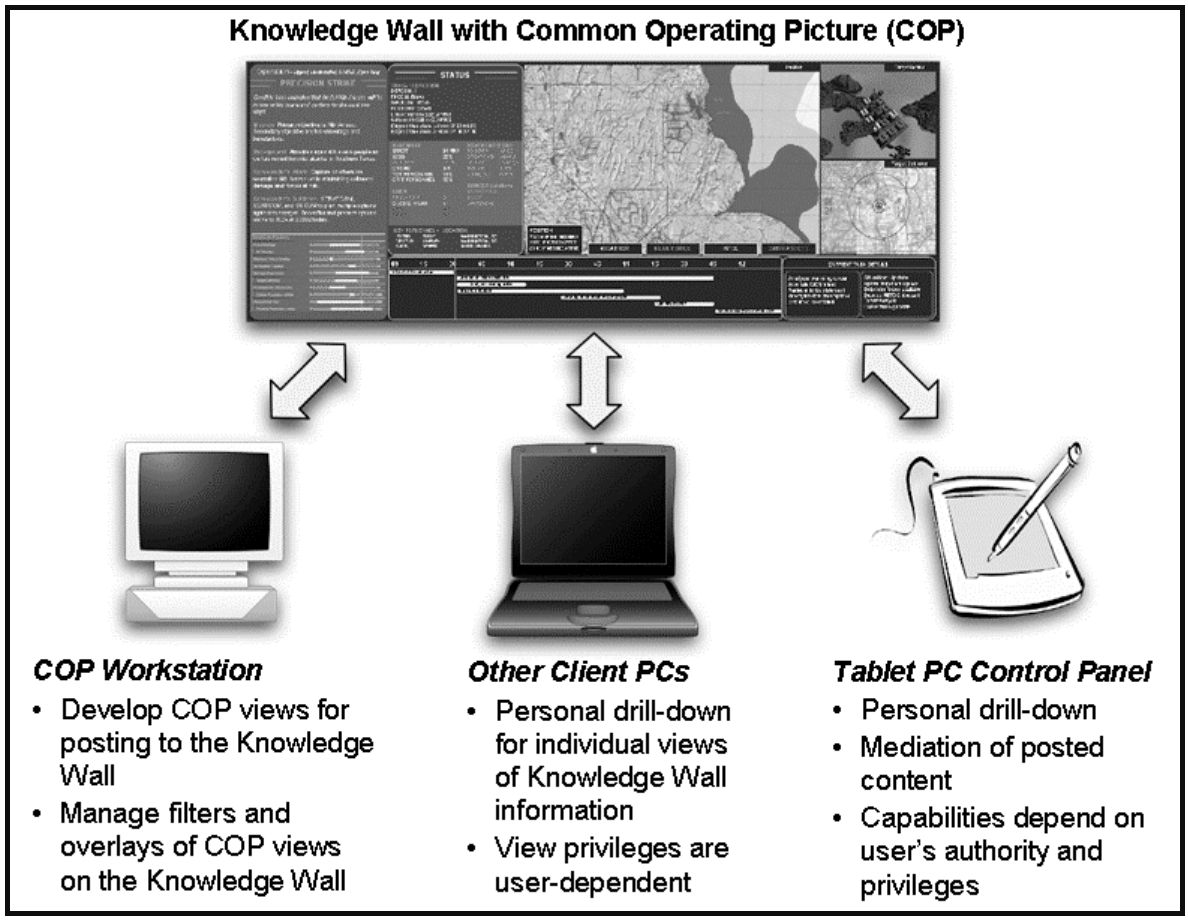

Figure 3: Components of the SIDEView Interactive Knowledge Wall System

Risk Assessment

A second key capability incorporated into the model is risk management. MITRE has long supported research and development in this area on behalf of government sponsors. The ARR model will draw on recent work, now in prototype stage, that provides prioritizing, displaying, and tracking of multiple-attribute risks. Called the Threat Event Assessment Model, this software system has these key features:

1. Clarity and traceability in generating and tracking threat assessments.
2. A flexible threat assessment method internal to the system.
3. Capability to generate and display threat event criticality rankings.
4. Generation of a Threat Situation Display that summarizes the current threat picture across all tracked threats
5. Analytic support for evaluating and making resource allocation decisions based upon the relative criticality of assessed threats

Figure 4 shows one type of threat situation display generated by ThreatNav, a component of the Threat Event Assessment Model. ThreatNav is an extension of RiskNav[4], a MITRE system that has seen extensive use in risk management settings. The chart on the left of the display shows assessed threats as colored boxes on a grid that scales consequences of occurrence on the vertical axis and probability of occurrence on the horizontal axis. The most significant threats then are those that fall toward the upper right. The status color of a box codes the degree to which the threat, as assessed, is being managed. Red indicates there are serious issues with the management of the threat; the other colors grade progressively to green, which indicates the threat is considered as under control. The box at the right of the display has controls for filtering and managing the threat chart; for example, one might display only the threats color coded as Red or Yellow, or just those with High Consequence and High Probability.

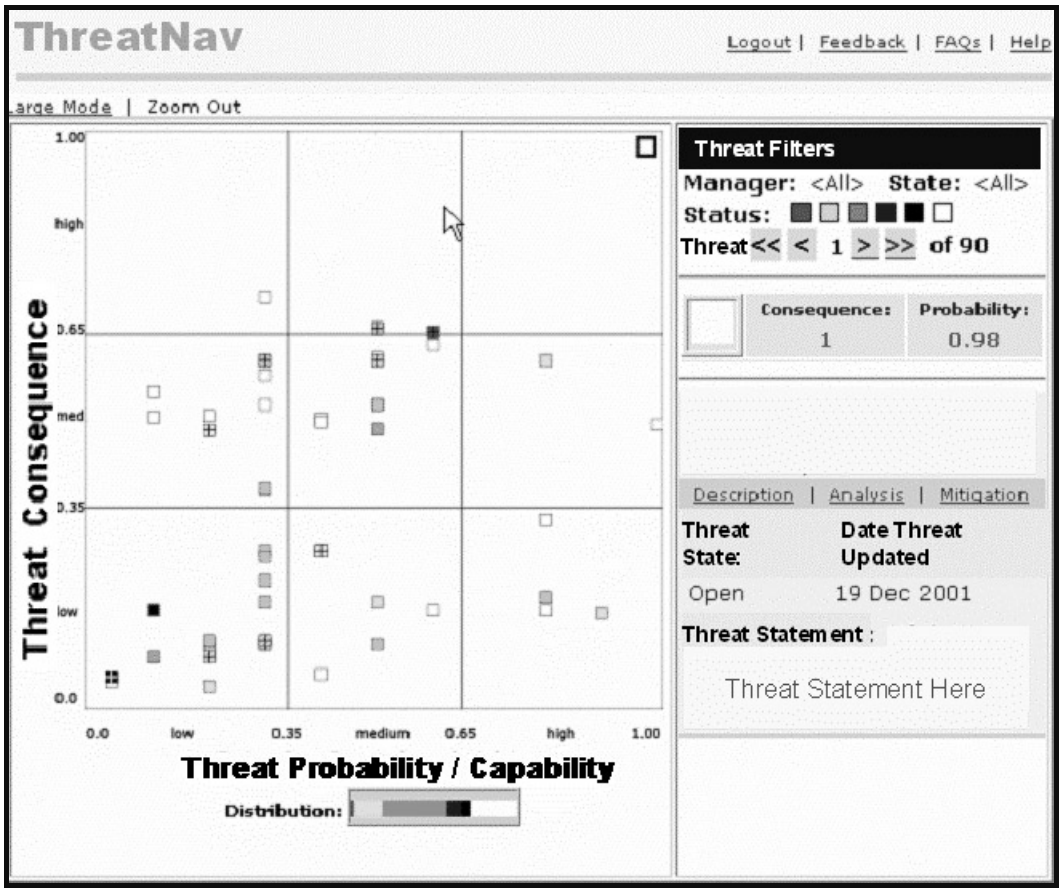

Figure 4: Prototype Threat Situation Display

Other Enabling Technologies

The initial ARR prototype will be constructed as a proof of concept. As such, it will be kept relatively simple, with SIDEView on a commercial collaboration platform and the Threat Event Assessment Model as centerpieces. However, the ARR model will provide an integration framework that facilitates incorporation of other applications.

The next step in developing the ARR model is to work with a set of organizations whose infrastructure protection concerns and issues provide an appropriate source of information to inform our own prototype efforts. The Port of Boston appears now to be the venue in which we will work. Our first steps will involve selecting a sub-set of port organizations and conducting an in-depth examination of information flows, data structures, and communication patterns so that the resulting ARR prototype reflects the reality of these organizations' security processes.

Further in the future, work will focus on enriching ARR with addition other applications. Examples of applications under consideration for integration with ARR are: Global Positioning; Geographic Information Systems; Mobile Wireless Access; and Sensors and Sensor Information Fusion.

ACKNOWLEDGMENTS

We thank Sandeep Mulgund, Norman Bram, and Paul Garvey of the MITRE Corporation, Arthur Faint, and the SAGE Group for helpful discussions.

REFERENCES

[1] Taylor, M. F. (2004) Emergency Management Technology – State of the Practice and Perspective on What's to Come, *Proceedings of the 2004 IEEE Conference on Technologies for Homeland Security*, Boston, MA

[2] Mulgund, S., Travis, A., Standard, J., Means, D., and Burgman, A. (2005) Shared User Interfaces for Dynamic Collaboration in Network-Centric Command Centers, to be presented at the *10th International Command and Control Research and Technology Symposium*, McLean, VA, June 2005

[3] Ragunath, M, Narayanaswami, C., Pinhanez, C. (2003) Fostering a Symbiotic Handheld Environment, *IEEE Computer*, September 2003

[4] Cho, C.C., Garvey, P.R., Gialombardo, R.J. (1997) RiskNav: A Decision Aid for Prioritizing, Displaying, and Tracking Program Risk, *Military Operations Research (MOR)*, 1997