



**Calhoun: The NPS Institutional Archive**

---

Faculty and Researcher Publications

Faculty and Researcher Publications Collection

---

2008-06

# Critical Infrastructure Protection Metrics and Tools Papers and Presentations

---

<http://hdl.handle.net/10945/51755>



Calhoun is a project of the Dudley Knox Library at NPS, furthering the precepts and goals of open government and government transparency. All information contained herein has been approved for release by the NPS Public Affairs Officer.

**Dudley Knox Library / Naval Postgraduate School  
411 Dyer Road / 1 University Circle  
Monterey, California USA 93943**

<http://www.nps.edu/library>

# CRITICAL INFRASTRUCTURE PROTECTION: METRICS AND TOOLS 5-7 JUNE 2008

PAPERS  
AND  
PRESENTATIONS



Center for Homeland Defense & Security  
Naval Postgraduate School



## Prioritizing assets in critical infrastructure systems

Dr. Hilda Blanco  
Professor and Chair  
Department of Urban Design and Planning  
University of Washington  
hblanco@u.washington.edu

### Abstract

Prioritizing is a fundamental task in capital facilities planning and finance. The protection of critical infrastructure systems, essential systems that underpin our society's "national defense, economic prosperity and quality of life" (President's Commission 1997), challenges the traditional methods used for prioritizing capital projects. The critical infrastructure systems identified in the various homeland security official documents are vast and complex systems which include among others, transportation, water supply, telecommunications<sup>1</sup>. The national interest in these systems is clear, protecting these systems from "incapacity or destruction". In effect, the national interest in these systems is to ensure that these systems are resilient and less vulnerable to potential threats, disasters, or accidents. The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (Office of the President 2003) requires government agencies as well as the private sector to identify and prioritize assets most essential to the nation's economic and social well-being. Traditional methods for prioritizing or selecting capital projects for investment fall into two categories, economic evaluation methods and more multicriteria approaches based on expert or departmental judgments, broad categories of need, urgency of need criteria, or program priorities, or goals. (Vogt 2004) Although the multicriteria methods could be applied to prioritize investments in critical infrastructures, such methods are difficult to apply to vast and complex systems often national in scale, and do not necessarily capture the systems or network aspects of the projects. In this paper, I first review and discuss major approaches to prioritization. I then focus on prioritizing system components and networks of critical infrastructures, focusing on Lewis's network theory (2006) approach to prioritize and invest for protection of nodes in critical infrastructure networks, and also review network interdiction approaches. Based on the limitations of the approaches reviewed, the final part argues that an enhanced systems analysis approach based on stock and flow diagrams would retain more information of the systems as systems and as networks than the more abstract network modeling.

---

<sup>1</sup> The following infrastructures have been identified as critical infrastructures for the nation: agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemical industry, postal and shipping. Office of the President. *The National Strategy for Homeland Security*, July 2002.

## 1. Introduction

Prioritizing is like thinking, everybody thinks they know how to do it, and, in the ordinary sense, we all do know. The issue for policy professionals who engage in this task is to set out and justify the rules or procedures we use to carry out this process on behalf of governments or corporate entities. Granted that each of us knows how to prioritize for ourselves, but how should public agencies or professionals working in such agencies prioritize, when faced with national or state or local agendas?

Prioritizing has received considerable professional attention in public policy. Often, prioritizing is seen to be part of the selection and evaluation of projects or programs for capital facilities planning and financing. As such, it is a primary function in public capital facilities planning (Vogt 2004). Since many critical infrastructures are capital facilities, its literature is most relevant.<sup>2</sup> In public finance, prioritizing projects takes the form of either a variant of cost-benefit analysis or more qualitative methods, ranging from experience-based judgment to sets of criteria based, for example, on need, or functional priorities. Often, some combination of such methods is used. These methods are acceptable at the local, state, and national levels to a large extent because the projects they are applied to are relatively well-bounded within a jurisdiction and/or a system. The idea of protecting or reducing the vulnerability of nation-wide critical infrastructures has unbound the process of prioritizing, and may call for more systems-oriented or network oriented approaches.

After a brief discussion of critical infrastructures and their characteristics, the paper reviews major approaches to prioritization, and their shortcomings when applied to critical infrastructure systems. I then focus on prioritizing projects from a critical infrastructure perspective as applied to system components and networks, discuss more systems-oriented quantitative methods and their limitations, focusing on the network theory approach to prioritize and invest for protection of nodes in critical infrastructure networks developed by Ted Lewis at the Naval Post Graduate School (2006), and also reviewing network interdiction approaches. Based on the limitations of the approaches reviewed, the final part argues that an enhanced systems analysis approach based on stock and flow diagrams would retain more information of the systems as systems and networks than the more abstract network analysis.

## 2. Critical infrastructures

The concept of critical infrastructures is a relatively new concept, defined in *Critical Foundations* (Pres. Commission Report 1997)<sup>3</sup> as *essential services that underpin our society's "national defense, economic prosperity and quality of life.* The report identified the following 8 critical infrastructures: transportation, oil and gas production and storage,

---

<sup>2</sup> In the field of public health, priority setting for healthcare has also received academic attention (Mullen and Spurgeon 2000; Mullen 2004).

<sup>3</sup> The report is also known as the Marsh report after Robert T. Marsh, the Chair of the President's Commission on Critical Infrastructures Protection that produced the report.

water supply, emergency services, government services, banking and finance, electrical, and telecommunications. This early definition and listing has been expanded over time by several acts and policies. The USA Patriot Act of 2001 defined critical infrastructures as “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters”<sup>4</sup>. The 2003 National Strategy for Homeland Security used the Patriot Act’s definition, and identified 11 sectors and 5 key assets. Added to the infrastructures identified in *Critical Foundations* were Agriculture and Food, Public Health, Defense Industrial Base, Chemical and Hazardous Materials, and Postal and Shipping.<sup>5</sup> When the Department of Homeland Security was established in 2003, critical infrastructures and key assets protection was one of its five mandates.<sup>6</sup>

What is it about each of these 11 sectors that makes them critical to the operations of the country or “that could be exploited to cause *catastrophic health effects or mass casualties* comparable to those from the use of a *weapon of mass destruction*”<sup>7 8</sup>? To be more specific, the various definitions have yielded 4 distinct criteria used to determine the inclusion of these infrastructures as critical. The Marsh report yielded two criteria, their essential role in national defense and in the nation’s economic security. The Patriot Act added public health and safety. The Homeland Security Act and the President’s National Strategy introduced the criterion of national morale. Thus, the four criteria used to identify critical infrastructures and justify their criticality are: essential role in national defense, economic security, health and safety and national morale. More recently, the *National Infrastructure Protection Plan of 2006* (NIPP) provided a framework for

---

<sup>4</sup> Patriot Act Section 1016 Critical Infrastructure Protection Act of 2001, section (e)

<sup>5</sup> Key assets are individual targets whose destruction could cause large-scale injury, or death or demoralize the country. The 5 key assets identified are:

- National Monuments and Icons
- Nuclear Power Plants
- Dams
- Government Facilities
- Commercial Key Assets (Major skyscrapers)

It is clear that the key assets identified are not infrastructures, most are not vital to the minimum operation of the nation, but they either have great cultural value, their loss would demoralize the country, or, as in the case of nuclear power plants, can create local disasters.

<sup>6</sup> The responsibilities of DHS include: intelligence and warning, border and transportation security, domestic counter-terrorism, critical infrastructures and key assets, defending against catastrophic terrorism, and emergency preparedness and response. 2002 Homeland Security Act.

<sup>7</sup> The Whitehouse, “Homeland Security Presidential Directive/Hspd-7” December 17,2003.

<http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html>

<sup>8</sup> Also useful to understand the justifications for these infrastructures is President Bush’s 2003 Presidential Directive/Hspd-7. In this directive, critical infrastructures and key assets targeted for enhancement are those that are vulnerable to terrorist attacks that could: cause “catastrophic health effects or mass casualties comparable to a weapon of mass destruction” (WMD); or impair federal agencies “to perform essential missions, or ensure the public’s health and safety”; “undermine State and local governments’ capacities to maintain order and deliver minimum essential public services”; damage the private sector’s ability to function and deliver essential services; “have a negative effect on the economy through cascading disruption on other critical infrastructures and key assets”; “undermine the public’s morale and confidence in our national economic and political institutions”.

developing sector specific plans, and outlined a general strategy for managing risk for critical infrastructures. The steps in the Plan's risk management strategy include: setting security goals; identifying assets, systems, networks and functions; assessing risk; prioritizing; implementing protective programs; and measuring effectiveness. Note that the NIPP applies the concept of prioritizing to countermeasures. The NIPP is a general framework and relies on sector-specific plans to make more concrete its goals and objectives, with due flexibility.

Critical infrastructure systems are recognized as being more critical and vulnerable due to their interdependencies, especially their increasing cyber interdependencies. This growing interdependency has increased their vulnerability to breakdown due to normal accidents, natural hazards, or intentional attacks, from terrorists or criminals. The figure below from the National Research Council Report (2002), *Making the Nation Safer*, is a depiction of the interdependencies of critical infrastructures. As you can see, electricity and telecommunications are mediating infrastructures for all the other systems, but the systems have additional interdependencies.<sup>9</sup>

**Figure 1. Critical infrastructure interdependencies**

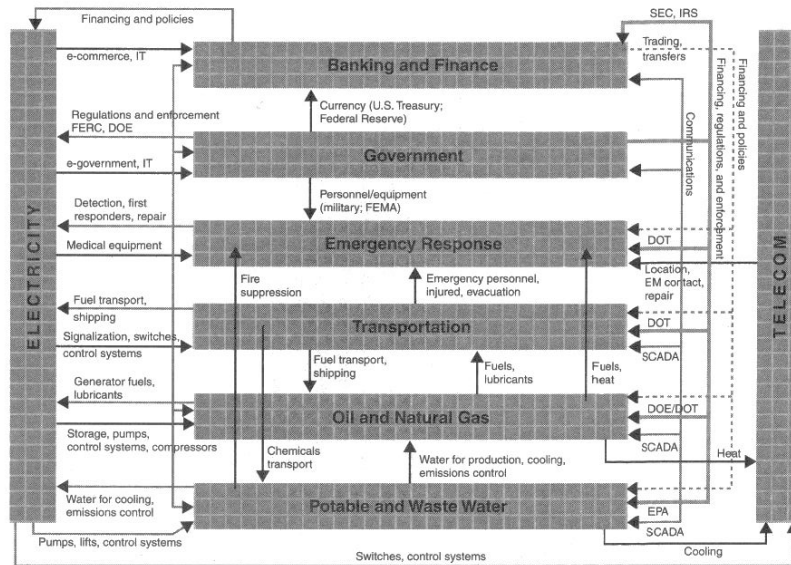


FIGURE 10.4 Critical infrastructure interdependencies. SOURCE: Heller (2002), by permission of the author.

301

Source: National Research Council (2002) p. 301

<sup>9</sup> See also Rinaldi, Peerenboom, and Kelly (2001) for a discussion of critical infrastructure interdependencies.

The difficulty of prioritizing projects in critical infrastructures stems from several reasons. First, critical infrastructures are complex systems. A system is a dynamic set of interdependent elements that interact with each other to produce a result or results. Critical infrastructures are complex systems in that they are composed of various types of elements, including technical or engineered elements, organizational, social, economic, informational, and natural, which interact in complex ways, and are interdependent on one another. They are also so vast, encompassing so many elements over great geographic regions that we cannot hope to protect every part of these systems. For example, in aviation, there are over 500 commercial airports, and close to 19,000 general aviation airports, and approximately 80 commercial carriers, including 14 major carriers (defined by at least \$1B in annual operating revenues). Just focusing on commercial flights, U.S. carriers in 2007 made 10.7 million domestic and international flights, and carried 769.4 million persons.(U.S. Department of Transportation 2008) In addition to the airports, and the airplanes and their personnel involved, the aviation system includes a complex air traffic control system, where air traffic controllers who rely on technical equipment as well as human judgment play a crucial role. Many of these systems are national, such as telecommunications, others are large regional systems involving several states, such as power. The vastness of these systems, given limited resources, makes it impossible to be comprehensive in trying to protect them. Instead, we need to be strategic. Note that a critical infrastructure is not just a technical or engineered system, but also includes organizational, economic, and social aspects.

Critical infrastructure systems are complex in themselves, and in their interdependencies. These systems are often what Perrow (1984) called coupled systems, that is, systems with more time-dependent processes (reactions are almost instantaneous); where the sequences are more invariant (for example, in a nuclear or chemical plant, things cannot be added later in the process). Typically, these systems have only one way to reach the production goals (a nuclear plant cannot produce electricity by shifting to coal or oil, but an oil plant can shift to coal); and they have little slack (quantities must be precise, resources cannot be substituted for one another).

As Lewis (2006) argues, we also lack sufficient technical knowledge of these critical infrastructures to understand how to protect them. Complicating this knowledge problem is the interdependency of these systems. As mentioned above, much of the new vulnerability of these systems is due to cyber interdependencies, as well as energy dependencies, which can result in cascading failures. A cascading failure is when a disruption in one infrastructure system causes a failure in the component of another infrastructure system. (Rinaldi, Peerenboom, and Kelly 2001) The 2003 Eastern Blackout is a good example of the interdependencies between the power and water systems and of a cascading failure. Cities like Detroit and Cleveland that relied on pumping for their water supply systems, lost their water supplies during the blackout. And the water systems took twice as long to restore as the power system.



## 2.1 Protecting Critical Infrastructures

The new public charge to safeguard critical infrastructure systems is, in effect, a charge to reduce the vulnerability of such systems to breakdown. Before 9/11, the vulnerability of critical infrastructure systems made us fear their breakdown due to accidents or natural hazards. After 9-11, the threat of terrorism gained center stage. In the risk analysis literature, risk is defined as severity of impacts times the probability of an event (Lowrance 1976). Vulnerability is often used interchangeably with risk, although there is much ambiguity in the use of the concept. In the hazards literature, vulnerability is often defined as “the susceptibility of resources to negative impacts from hazard events” (NOAA 2008). In the climate change literature, vulnerability has evolved into an integrative concept, and is seen as a function of susceptibility, exposure to a hazard, and adaptive capacity:

Vulnerability is the degree to which a system is susceptible to, and unable to cope with, adverse effects of climate change, including climate variability and extremes. Vulnerability is a function of the character, magnitude, and rate of climate change and variation to which a system is exposed, its sensitivity, and its adaptive capacity. (IPCC AR4 WG II 2007, 883)

The NIPP (2006, 35) identifies risk as a function of consequence, vulnerability and threat:

$$R = f(C,V,T)$$

where consequence is defined as the negative impacts on public health and safety, the economy, public confidence in institutions and the functioning of governments, etc.; vulnerability is defined as likelihood that an attribute of a component of a system renders it susceptible to fail due to any type of hazard; and threat as the likelihood that a particular asset will suffer an attack or an incident.

The concept of resilience is widely used as the opposite of vulnerability, as the “flip side of vulnerability—a resilient systems or population is not sensitive to climate variability and change and has the capacity to adapt.” (IPCC TAR WG II 2001, 89) Four aspects of disaster resilience have been identified (Tierney and Bruneau 2007): a) robustness—the capacity “to withstand disaster forces without significant degradation or loss of performance; b) redundancy—the extent to which there are substitutes to accomplish the function of a system or element of a system, in case a system fails; c) resourcefulness—“the ability to diagnose and prioritize problems and to initiate solutions by identifying and mobilizing material, monetary, informational, technological, and human resources; and d) rapidity—the ability to restore system performance “in a timely way, containing losses and avoiding disruptions.”

Prioritizing the critical elements of infrastructure systems to reduce the system’s vulnerability to breakdown from natural or intentional causes thus requires identifying their contribution to the system’s performance, the major hazards they are exposed to, their susceptibility to specific hazards, and the system’s adaptive capacity. Setting priorities for critical infrastructures protection could also be seen as a task to identify the least resilient elements of a system, in which case resiliency could be gauged, following

Tierney and Bruneau, in terms of an element's robustness, the system's or element's redundancy, the resourcefulness or adaptive capacity of the organization or community involved, and the rapidity of restoration.

### **3. Prioritizing/selection of projects for investment**

Traditionally, the major criteria used in capital facilities planning and finance are two, economic efficiency, and public or policy preferences. In consequence, traditional methods used to select projects for planning and budgeting fall into two main categories, economic evaluation methods, and methods that employ multi-criteria and Likert-type scaling measures.

#### **3.1 Economic Selection Methods**

The major economic evaluation methods include cost-benefit, net present value, and cost-effectiveness analyses. Cost-benefit analysis is a comparative process that analyzes the potential consequences of several projects, and provides a process for choosing among them. Cost-benefit analysis relies on a prior selection of projects for comparison. It does not provide a rule for identifying projects for comparison. This type of economic evaluation consists of listing the relevant costs and benefits of projects, tangible and intangible, although in practice, it often only includes tangible costs and benefits. In a benefit-cost analysis benefits and costs are translated into monetary terms, and then these benefits and costs are aggregated. Once aggregated, an appropriate discount rate is applied to the total benefits and the total costs. Projects are then compared and the project with the higher benefit/cost ratio is selected. Net present value is benefit-cost analysis without calculating the ratio, the total costs are subtracted from the total benefits for each project and the net present values of the projects are compared. Cost effectiveness is a technique where the benefits or the costs are held constant, and the comparison focuses on the project that provides the most benefits for a set cost, or the most cost-effective project for a given benefit. (Aronson and Schwartz 2004; Stokey and Zeckhouser 1978)

In the context of prioritizing for critical infrastructure systems protection, cost-benefit analysis and other economic evaluation techniques can be useful once an element of a system has been identified as vulnerable. These types of analyses could then be employed to evaluate the economic viability of alternative projects for hardening or making more resilient a specific component in a system. And this is the role that vulnerability assessments of critical infrastructure systems assign to economic evaluation techniques, as we discuss in Section 4 below.

#### **3.2 Multi-criteria Approaches to Prioritizing Capital Projects**

Although some local and state governments use economic evaluation methods to select projects, most rely on multi-criteria methods for prioritizing capital projects. (Calia 2001; Vogt 2004; Millar 1988) Criteria typically include government objectives, which are more or less the outcome of representative democracy processes, and thus,

these methods are based on choices concerning public goals. According to Vogt (2004) in his textbook on capital budgeting and finance, these methods range from the experience-based judgments of experts, and departmental priorities set by department heads to the use of rating systems to set priorities for the jurisdiction as a whole based on:

- Broad Categories of Need. In this type of ranking system, projects are rated high or *must do*, medium or *should do*, and low or *could do* priority. A type of need prioritization scheme can also use a numeric or ordinal scale to assign ratings for high, medium and low priorities. (Vogt 2004, 92-94)

- Urgency-of-need criteria—This type of ranking system uses criteria such as: meets legal mandates, removes or reduces a hazard, advances the governing board’s goals and objectives, improves efficiency, maintains standard of service, etc. (Vogt 2004, 94-97)

- Weighted rating of urgency-of-need and related criteria—A weighted rating system can also be applied to an urgency-of-need set of criteria, such that each criterion, such as “meets legal mandates” can be rated or scored along a numerical scale from 0 a “clearly no” rating to a 6, a “clearly yes” rating. In addition, each criterion can be assigned a different weight, depending on the priority assigned to the various criteria, e.g., “meets legal mandate” can be assigned a weight of 40%, and the score can then be multiplied by the weight of the criterion, e.g., in the case of a project that meets legal mandates with a score of 5, and a criterion weight of 40%, its weighted score would be 2; while a project that reduces a hazard can be scored a 5, but with a criterion weight of 30%, its weighted score would be 1.5. (Vogt 2004, 97-111)

- Program priorities, goals, and service needs—while “meeting program goals” can be one of several criteria included in the criteria discussed above, some local governments select projects based solely on whether projects meet program priorities, goals and policies of the governing board, which are often expressed in a master plan or strategic plan or the executive’s policy agenda. (Vogt 2004, 111-115).

Many of these multi-criteria methods are based on a scaling system, which can be simple or weighted. In such cases, the public facility systems and their performance are reduced to criteria; the criteria are prioritized and sometimes weighted depending on a locality’s policy preferences; projects are scored according to the scales used, and their weights are calculated. Capital allocation priorities in a jurisdiction are then decided on the basis of the weighted score assigned to the projects.

#### **4. Multi-criteria approaches for prioritizing in critical infrastructure systems**

Prioritization can be applied at several stages in planning processes. The NIPP, for example, outlines a process where prioritizing occurs after risk analysis and is primarily applied to setting priorities for implementation. Calling for prioritization at this stage, and failing to identify the need to prioritize assets ignores the vast nature of infrastructure systems, and the need to prioritize elements prior to vulnerability or risk assessment. The sector-specific plan for water systems identified this issue as a concern and added a component of infrastructure screening to their plan, noting that:

Given the large number of Water Sector utilities throughout the Nation and the limited resources available to address their security, the objective of the RAMCAP [the NIPP's Risk Assessment Methodology for Critical Assets Protection] process is to prioritize at the national level those sector assets that warrant more in-depth risk analysis. The entire sector, especially owner/operators, may benefit from coordination within the sector on development of a screening process to determine the need for detailed risk assessments. Risk assessments are iterative; therefore, exploring development of screening methodologies could help identify assets that are significant enough to require further assessment. (US DHS and US EPA 2007, 59)

The transportation-specific plan followed NIPP instructions, and applied the concept of prioritization to countermeasures, but the plan also adds a filtering step to assess assets for criticality (2007, 57) right after the development of the asset inventory.

In this article, we are focused on the initial screening of the vast inventories of critical infrastructure systems into a small set of assets or components of a system in order to facilitate further analysis of the vulnerability of such assets to break-down or attack. In this context, several federal and state agencies have turned to multi-criteria scaling systems to identify the most critical components of systems. A good example is the method developed for the American Association of State Highway Transportation Officials (AASHTO) prepared by SAIC (2002) which was developed to assist state departments of transportation (DOT) to prioritize elements of their transportation infrastructures for critical infrastructure protection.

SAIC's guidebook lays out a vulnerability assessment with three major parts: identifying and prioritizing assets or *criticality analysis*; conducting a *vulnerability assessment*; and *post assessment plans*—or planning for implementation of countermeasures. Priority setting is the first part of this process, and it includes identifying all critical assets in the form of a list, establishing and assigning values to critical asset factors, and prioritizing the critical assets, which results in a criticality score for each asset. The second step, conducting the vulnerability assessment, calls for characterizing the threat, identifying exposure level, and scoring the asset vulnerability. This step yields a vulnerability score. The next step calls for the criticality (X coordinates) and vulnerability scores (Y coordinates) for each asset are plotted in a matrix, e.g., if an element of a system has both high criticality and vulnerability scores, it would be plotted in Quadrant I, but if an asset has low criticality and high vulnerability, it would be plotted in Quadrant IV. The final step, the post assessment plans, examines countermeasures to high priority critical assets, and assesses their effectiveness. According to the SAIC handbook, the last step may include conducting cost-benefit analyses and tradeoff studies, as well as actual implementation of countermeasures.

Focusing on the criticality analysis, which establishes priorities, the method begins with a list of assets, which include infrastructure, facilities, equipment, and personnel. The SAIC Guide then provides a list of 14 critical asset factors (the multi-criteria), their value and descriptions for each of the factors. Critical asset factors

include: ability to provide protection, relative vulnerability to attack, casualty risk, emergency response function, functional importance. The factors or criteria are assigned a binary value, which ranges from 1-5 if the factor applies, or 0, if the factor does not apply. The Table below illustrates the method, where each of the letters stands for a criterion or factor. The higher the total score, the more critical the asset.

Table 1. Illustration of SAIC Method for Scoring Criticality of Critical Infrastructure Assets

Critical Asset	Critical Asset Factor														Total Score
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	
Asset 1	1	2	5	1	3	3	5	0	5	4	1	5	2	1	38
Asset 2	1	0	5	1	3	3	0	5	5	0	1	0	2	0	26
Asset 3	0	2	0	1	3	3	5	5	5	0	0	5	0	0	29
Asset n	1	2	5	1	3	3	0	0	0	4	1	5	2	0	27

Source: Modified from SAIC Report to AASHTO, A Guide to Highway Vulnerability Assessment (2002), p. 14.

This scoring method is a weighted one, for example, factor or criterion C, the possibility of casualty risk is scored a 5, while factor D, environmental impact, scores a 1, and factor M, functional importance scores a 2. As this illustration makes clear, the value of this approach rests on several things, including, whether the right criteria were included, and whether the appropriate weighing was assigned to each of the criteria. (SAIC 2002, 9-14)

The risk filtering, ranking, and management (RFRM) method developed by Haimes, Kaplan, and Lambert (2002a; Haimes 2004) aims “to identify, prioritize, assess, and manage scenarios of risk to a large-scale system from multiple overlapping perspectives.” (Haimes et al. 2002a, 384). It takes into account the multiple perspectives of different stakeholders involved in complex systems and utilizes multicriteria evaluation. It has been applied to filtering over 900 sources of risk to U.S. Army telecommunications systems information assurance (Haimes et al. 2002b), to setting priorities for protecting bridges against terrorist attacks (Leung, Lambert, and Mosenthal 2004) and more recently to protecting critical infrastructure assets in the Army (Anderson, Barker, and Haimes 2008). Although the 8-phase method<sup>10</sup> is focused on risk scenario identification, in their application to Army assets, Anderson and his associates have modified it to apply more directly to assets or elements of systems. The list of critical assets resulting from the Army study is based on two major elements, the criticality of assets to meeting Army goals, and the vulnerability of assets to a particular hazard. RFRM uses a hierarchical holographic model (HHM) to represent the

<sup>10</sup> The eight phases of RFRM are: I) scenario identification through hierarchical holographic modeling (HHM); II) scenario filtering based on scope, temporal domain and level of decision making; III) Bi-criteria filtering and ranking; IV) multicriteria evaluation, criteria related to the system’s resilience, robustness, and redundancy; V) quantitative ranking; VI) risk management options are developed and evaluated; VII) safeguarding against missing critical items, continuous review and reevaluation; VIII) operational feedback

characteristics and attributes of a system from multiple aspects, such as Army organization, core competencies, security, challenges, defense and civil infrastructure sectors, geography, temporal, etc. The second step in the process calls for scoping the asset prioritization task. This scoping process is based on a specific threat scenario, e.g., an earthquake, and a specific decision maker, e.g., an Army Material Command Commander, with specified objectives, e.g., deployment readiness, and affected infrastructure sectors, e.g., electrical supply. The commander in such an exercise is concerned with identifying the infrastructure sectors vulnerable to an earthquake that could keep his command from being ready for deployment (Anderson, Barker and Haimes 2008, 7). In the modified RFRM used in the Army study, assets are filtered through the Army's Balanced Scorecard Method (Kaplan and Norton 1992), that is, the set of criteria used to judge critical assets are the core competencies and objectives for the various levels of Army organization.<sup>11</sup>

Assets can then be mapped onto the scorecards. The next step in the method is meant to define the extent to which the assets are required to meet the objectives of the scorecard. This is done through the use of a risk-severity matrix for criticality, based on measures of likelihood and consequence or through an impact matrix, where assets are located in a matrix according to the scorecard objectives they are associated with and the severity of impact they would have on the scorecard objective. For example, in case a risk-severity matrix is used, if loss of Asset 5 is almost certain to cause the failure a scorecard objective, then the element is designated as having high criticality. In case an impact matrix is used, assets with high criticality are assets that have a high impact score and that impact several scorecard objectives.

Unlike the SAIC report, the list generated at this point in the methodology is not ordered or ranked but just bulleted, although in a later step in the process, priority weighting may be added. Similar to the SAIC methodology, the Army study uses the criticality list as input for its vulnerability assessment. Two tools are used in the vulnerability assessment, a risk-severity matrix that is applied to the attributes possessed by an asset, not the asset itself, e.g., throughput, and 14 criteria that relate the ability of a threat scenario to prevail over four defensive properties, resilience, redundancy, robustness, and security.<sup>12</sup> Once the list of vulnerable assets has been produced, an overall prioritized list can be generated by combining the critical asset list with the vulnerable asset list in a matrix, such as depicted in Table 2 below.

Table 2. Modified RFRM Prioritized List of Assets

---

<sup>11</sup> . This set of criteria corresponds to the prioritizing approach discussed in the section above as the “program priorities of the governing board” approach.

<sup>12</sup> The 14 criteria are: undetectability; uncontrollability; multiple paths to failure; irreversibility; duration of effects; cascading effects; operating environment; wear and tear; hardware/software/human/organization interfaces; complexity and emergent behavior; design maturity; singularity; accessibility; unaffordability.

Vulnerable Asset List	Critical Asset List	
	High	Medium
High	Asset 2, Asset 7	Asset 6
Medium	Asset 4	Asset 9
Low	Asset 1	Asset 3

Source: Modified from Anderson, Barker and Haines (2008)

The highlighted set of assets identifies the prioritized list of assets. Note here that the criterion for inclusion in the priority list is ranking high in either the critical or the vulnerable asset list. The remaining steps of the RFRM method include risk management, i.e., identifying steps that can be taken to: reduce vulnerability; the trade-offs; and the impacts of current decisions on future options. In addition, RFRM includes feed-back loops to review the findings, as well as to improve the tools.

#### 4.1 Strengths and Weaknesses of Multicriteria Approaches

Multi-criteria approaches are popular for several reasons. They allow stakeholder involvement in the selection of criteria, their scoring and weighting. They do not require extensive calculation, simulation, or modeling, and thus, they make possible widespread application of the criteria by many individuals without much training, since criteria are simple to understand. But as we reviewed above, multi-criteria systems can range from simple, e.g., the SAIC approach, to more complex, e.g., the RFRM approach which requires a large set of inputs. In general, multi-criteria approaches, if standardized across the country, can facilitate comparison across jurisdictions.

Although multi-criteria approaches can be sophisticated, in the analytic process, these methods lose information of the system as a system. Although the RFRM approach emphasizes the importance of the state variables of a system or its components to the concept of vulnerability (Haines 2006) the interconnectedness of the components of a system is lost in these approaches, as well as the spatial character of critical infrastructure systems. In a similar way, in these methods, criteria can identify interdependence, but they fail to capture the topology of interdependence. Critical infrastructure systems are networks, where there are discernible hubs and connections among hubs. The multi-criteria approaches do not necessarily address the network aspect of these systems.

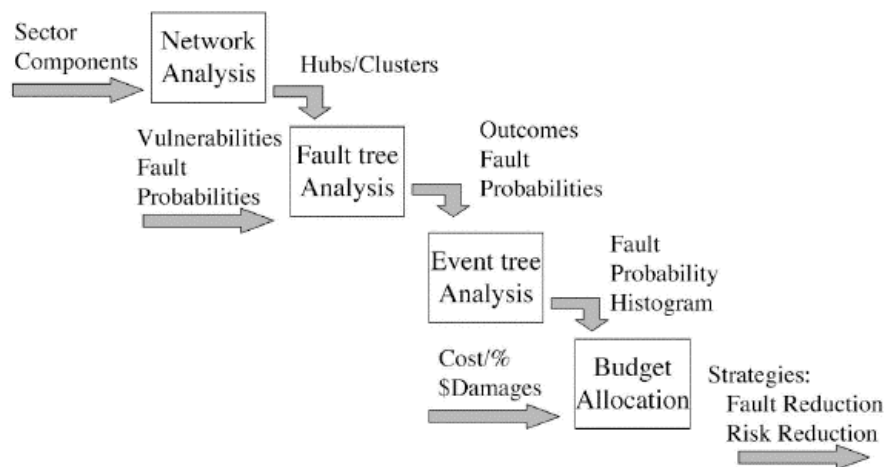
#### 5. Network theory approach applied to critical infrastructures

Ted Lewis (2006) has developed a network theory-based approach to prioritize critical infrastructure components or assets and conduct vulnerability assessments. His text on critical infrastructure protection outlines a vulnerability assessment process, see Figure 1, which includes a network analysis to determine priorities in critical assets within an infrastructure system, followed by fault tree and event tree analyses for the critical assets of a system, and concluding with budget allocation algorithms that can minimize fault or risk. Fault tree and event tree analyses are part of a suite of risk analysis tools used by safety and reliability engineers.

Fault tree analysis is a logical, structured, and graphical process to identify potential causes of system failure. In fault-tree analysis, a logical tree is constructed with the failure of the system at the top of the tree, threats at the bottom, and a chain of causes leading from the threats to the failure connected by logic gates (AND or OR). Event-tree analysis is a logical structured process to determine the consequences of an initiating event and the expected frequency of each consequence. For example, a pipe breaking in a nuclear power station may have many consequences ranging from a very small release of radiation (no significance) up to a very large release of radiation (catastrophic). Event trees model these initiators and consequences, and determine their frequencies. These traditional risk analysis approaches and techniques typically aim to identify all exposures to all components of a system, such as a nuclear power plant, that may be at risk or vulnerable and identify all threats. The results of these analyses then yield probabilistic risks, and depending on the risks the major components that need to be protected are identified.

Since critical infrastructure systems are vast, Lewis’s method begins by narrowing down the potential exposures to a few assets of a network. This reduces the assets of a system that need to be analyzed by orders of magnitude, and makes it possible to use the traditional techniques of safety and reliability engineering.<sup>13</sup>

Figure 1. MBVA Process: After Taking Inventory: Perform Network, Fault tree, Event tree Analysis, and Budget Allocation.



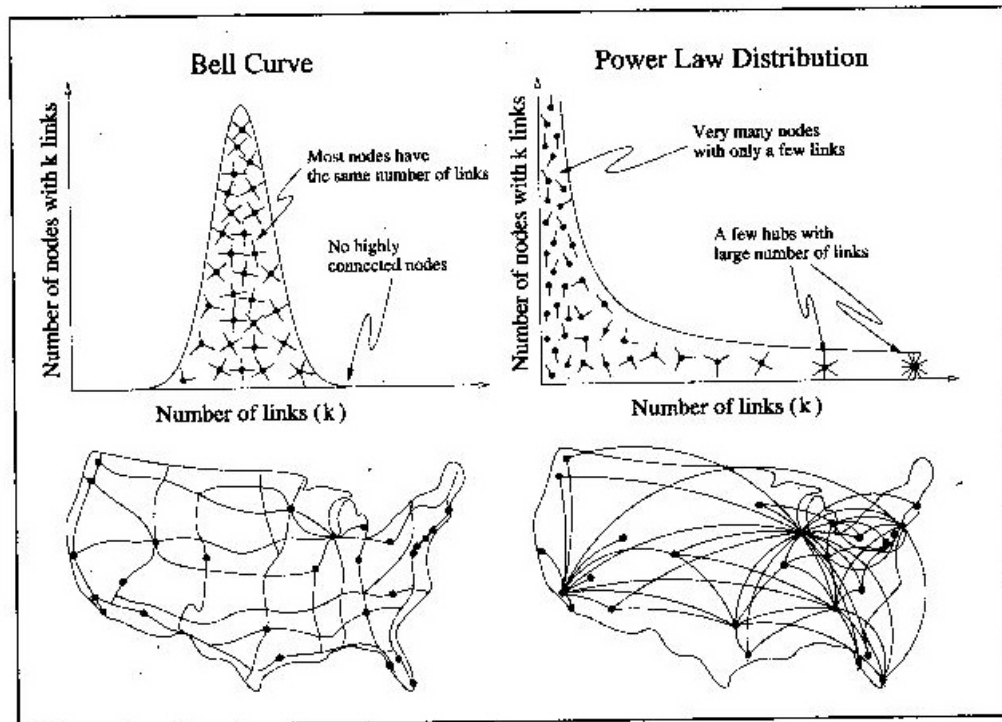
Source: Ted Lewis. 2006. *Critical Infrastructures Protection in Homeland Security*. P. 110. Wiley and Sons.

<sup>13</sup> Notice also, that in addition to the assets identified in the network analysis, key vulnerabilities or threats to such assets as well as the probabilities of the threats occurring are also inputs for the fault tree analysis.



## 5.1 Using Network Theory to Prioritize Assets in Critical Infrastructure Systems

Lewis's network theory approach is based on recent work on non-random networks, especially scale-free networks (Barabasi 2002) but also small worlds networks (Watts and Strogatz 1998). Network theory is a branch of complexity theory, and initially its focus was on how dynamic, random, non-ordered systems can attain ordered states or self-organization through the application of simple rules. Its mathematical origins date back to Euler's graph theory<sup>14</sup>, which modeled systems as nodes and their links to solve topological problems. More recently, since the 1960s, sociologists, such as Milgram (1967), and Granovetter (1973) have revived the use of network theory through algebraic methods. Lewis's work is based on Barabasi's non-random network theory.



Source: A.-L. Barabasi. 2003. *Linked: How Everything is Connected to Everything Else and What it Means for Business, Science, and Everyday Life*. P. 71, PLUME Cambridge, MA

Barabasi's contribution to the mathematical theory of networks, partly through his analysis of the Internet, was to identify a type of network where the linkages are non-random, where just a few hubs have a very high degree of interconnection, and most

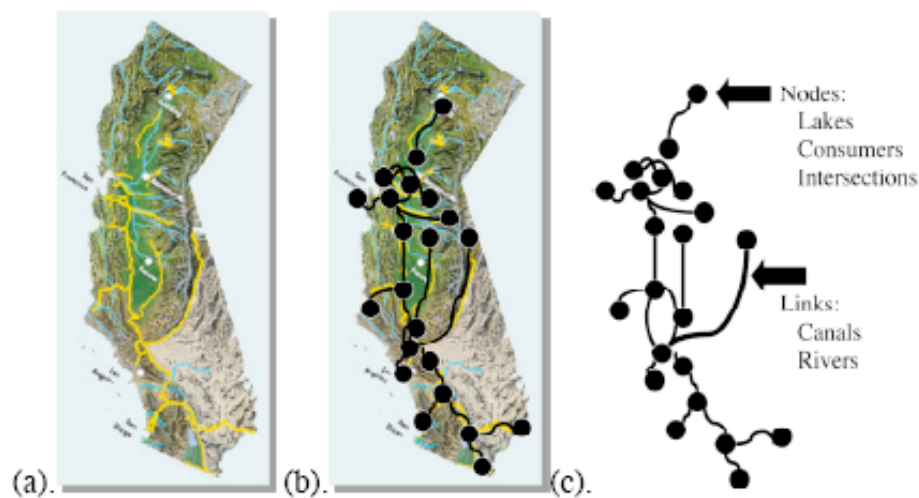
<sup>14</sup> Euler was the foremost mathematician of his time (1707-1783). Euler's inspiration for his invention of graph theory was the popular problem that the 7 bridges of Koningsberg posed to its citizens: Was there a way to start at one of the bridges and cross all of them without crossing anyone twice? Euler's great innovation in 1736 was to graphically portray the land masses as points or nodes and the bridges as links between the nodes. (Barabasi 2002, 9-13; Lewis 2006, 41)

others are sparsely connected in the network. He calls these non-random networks with highly linked hubs, scale-free networks. The figure above compares a random network characterized by a normal distribution of linkages to a scale-free network that is characterized by a power law (that is the histogram drops off quickly as  $k$  increases).

Non-random network theory is appropriate for modeling critical infrastructure systems, since these systems typically have a concentration of assets, which can be modeled as critical nodes or hubs, and the distribution of linkages among nodes are non-random, either scale-free or small world. Small world networks are non-random networks whose distributions do not follow a power law. Typically, these are networks with the following characteristics: a large number of nodes; sparse, i.e., the average node degree of connection is much smaller than the number of nodes; decentralized, i.e., no dominant nodes; highly clustered—forming neighborhoods; and, connected, i.e., any node can be reached by a finite number of links (Watts 1999).

The application of network theory to a critical infrastructure system provides a simple procedure to determine whether an infrastructure system is random, scale-free, or small world. First, the assets and links between the assets are identified on a map. Then, the assets are characterized as nodes and the linkages as links on the map. In the example Lewis uses of the California aqueduct in the figure below, the nodes are lakes, consumers, and intersections, and the links are canals and rivers. Finally, the mathematical model of nodes and links is transferred to a graph, where the topological features of the links are preserved (3c in the figure).

Figure 2. A Mathematical Graph is used to Model the California Aqueduct as a Network. Map of California Aqueducts, (b). Network Nodes and Links Layered on the California Map, and (c). Network Model of Aqueducts as a Graph.



Source: Ted Lewis. 2006. *Critical Infrastructures Protection in Homeland Security*. P. 80. Wiley and Sons

Once the graph model has been developed for a system, a simple test can be carried out to determine whether a system is random, scale-free or small world network. The test consists of preparing a histogram of the distribution of the degree of linkages for the nodes in the system. If the degree of linkages follows a normal distribution, then the system is random; if it is a power law distribution, then it is a scale-free network; if there are clusters in the distribution, then it is a small world network. This test provides a prima facie rule for prioritizing critical infrastructure assets or components within a system. If a network has a few hubs with a high degree of connectedness, then the system is vulnerable to cascading failures at the nodes. Thus, the network analysis reveals the most critical hubs in the system, where protection and investment measures can best protect the network from cascading failures. Lewis's approach provides convincing simulations of how attacks in different hubs can propagate shutting down the system quickly (see the accompanying software to Lewis's text). As indicated, the network analysis carried out to prioritize hubs is only the first part of Lewis's Model-Based Vulnerability Analysis. Once the critical hubs are identified, fault tree and event tree analyses are carried out for the major threats to such hubs.

The process for identifying the critical nodes in a system is, thus, three-fold: identify the nodes and linkages in a system; graph the nodes and linkages; and, prepare a histogram for the degree of linkage of the hubs. If the histogram reveals a scale-free or small world network, then the critical hubs are the hubs with the greatest degree of linkage. This prioritizing method also has a clear policy directive, i.e., protect the hubs with the greatest degree of linkage. The next section illustrates the method.

## **5.2 Testing Network Analysis as a Prioritizing Method: The Interstate Highway system as a scale-free network**

In his *Critical Infrastructure Protection* text, Lewis analyzes several systems, such as, power, telecommunications, and water in depth using his new method. Although he does not cover transportation in depth, Lewis does discuss its network-like characteristics, and the transportation sector is a good sector to test the method on, since some transportation systems lend themselves easily to such analysis and others do not. Lewis uses the Interstate Highway system as an example to illustrate network analysis, and identifies cities with 6 or more links to the Interstate Highway system. Chicago is the winner with 10 such links, with Indianapolis and Dallas/Fort Worth with 7, and 6 other cities with 6 links. Most major cities have two links, one segment going into the city and another exiting, and the distribution follows more or less a power curve. (Lewis 2006, 90-91)

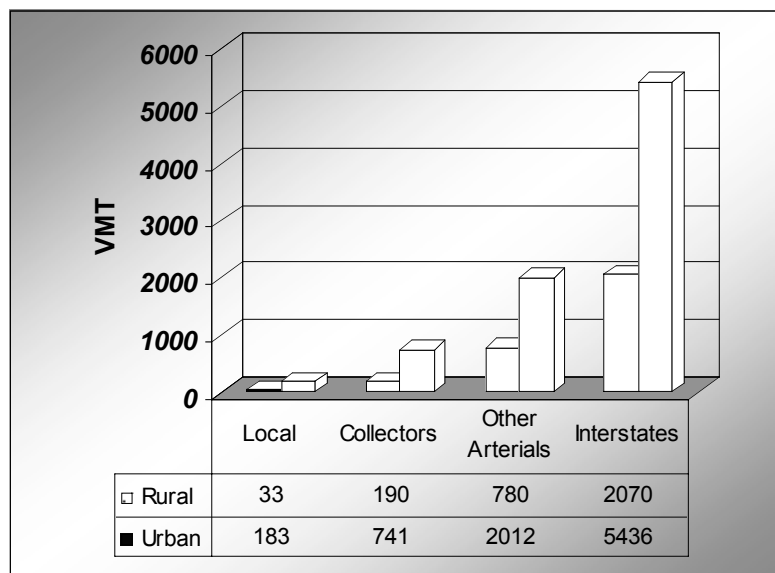
The network analysis methodology applies well to rail systems, because, in rail systems, stations can be interpreted as hubs, and rail lines as connectors. It is a bit more difficult to apply to road systems. What are the nodes in a road system? Lewis points out that segments of roads should at times be interpreted as nodes (Lewis, Chapter 5), but in the Interstate Highway network example above, cities have been interpreted as nodes. In this case, Seattle has four links to Chicago's 10. Does this interpretation lead us to see Chicago as most vulnerable and Seattle as less vulnerable given their degree of

connectedness? Would the method lead us to invest more in protecting the interstate highway system in Chicago than the one in Seattle? But Seattle’s lack of redundancy renders it more vulnerable than Chicago. This suggests that the criterion of degree of connectedness used in network analysis needs to be supplemented with a criterion of lack of redundancy. Thus, the choice in interpreting which are to be the nodes versus the links in the network is a crucial choice.

The interstate example also raises the issue of scale, i.e., whether cities can be interpreted as hubs of a highway system. Cities, such as Chicago, are geographically too large, and the 10 interstate highway connections within Chicago are not all concentrated within one segment of road. Within this large city, there are multiple junctures where two to three of the interstate highways are linked. In addition, is it appropriate to consider the interstate highway systems without taking into account the larger road system within a region? The interstate highway system is one element, although a vital one, in regional and national road systems. Within metropolitan areas, they are linked to arterial roads which serve similar functions as the interstate system, and sometimes have similar capacity. In general, in U.S. metropolitan areas, the road system is typically a highly redundant system.

The road system as a whole is an intentional scale-free network, as the histogram of vehicle miles traveled (VMT) per lane mile in the figure below demonstrates. The hierarchical system of road classification, the result of functional and administrative objectives, is the intentional element that makes the road system a scale-free network. This intentional hierarchy of roads leads us to the rule of thumb for road infrastructure, first protect highways, then major arterials. This is one of the major screens that the federal government has used to designate the National Highway System.

Figure 3. Rural and Urban VMT per Lane Mile (in thousands) by Functional Road Class, USA 2003



Source: Adapted from Bureau of Transportation Statistics, Table 1-33. At: [http://www.bts.gov/publications/national\\_transportation\\_statistics/2004/html/table\\_01\\_33.html](http://www.bts.gov/publications/national_transportation_statistics/2004/html/table_01_33.html)

### **5.2.1 Strengths and weaknesses of Lewis's network theory approach to prioritizing**

The major strength of Lewis's network analysis approach to prioritizing is the simple test of node degree it employs for identifying critical hubs in complex networks. This test requires minimal spatial information about a system readily available to designate nodes and links, and the training required to apply such a test is moderate. Also, the graphic display is convincing. Such a test is most useful for scale-free networks, but less so for small world networks (Grubestic et al. 2008). In addition, the software Lewis developed to illustrate his network approach provides convincing simulations of how the network is affected by attacks to different nodes in a system.

Lewis's network analysis approach to prioritizing encounters several challenges, however. Fewer links for transportation or other systems may mean more, rather than less vulnerability. As in the case of the interstate highway connections in Chicago and Seattle, lack of redundancy may trump degree of connectedness. Further, when the node is geographically too large, as in the case of Chicago and the interstate system, the analysis may need to be done at a smaller scale, i.e., to identify vulnerable spots within a node. In general, network analysis at a regional or smaller scale may require subcomponent analysis, such as chokepoints, e.g., tunnels, bridges, vs. entire highway segments. Also, when a system is interconnected with another system, as the interstate highway system is interconnected with local and regional road systems, it may be more strategic to select the more inclusive system to determine priorities.

In critical infrastructures which are supply chains, such as oil or natural gas systems, the sequence or order or direction of flow is important, and the source node or hub may be more critical than the degree of its linkage within a system. For example, in the Southern California Kinder Morgan oil pipeline transmission system, the Watson pipeline is the source pipeline connected to more than 10 refineries in the Los Angeles Basin. Network analysis shows Watson to have two pipeline linkages, while Colton and Niland, internal segments of the pipeline, have 3 linkages. Using a degree of node connectedness indicator would lead us to consider Colton and Niland somewhat more or as critical as Watson<sup>15</sup>, yet if Watson were to fail, then the system as a whole would be brought down, whereas if Niland or Colton were to fail, only part of the system would fail. In general, where the connectedness or flow of a system is important, then other network indicators may be necessary to identify network asset priority.

## **5.3 Interdiction network approaches**

---

<sup>15</sup> Lewis, Chapter 10. Lewis makes up for this by designating a higher value for the Watson pipeline, and a higher damage cost in the fault-event tree analysis. Having to compensate for the lack of guidance from the network analysis indicates that network analysis less useful as a prioritizing tool for this type of system.

Military strategists have used network theory to minimize the disruption or *interdiction* of critical nodes or links in a supply network or chain. When interdiction occurs, the destruction or disabling of a node or critical arc can disrupt the network's topology and performance. Interdiction theory can be used to determine how best to cut off enemy supplies by taking out a small number or the least number of nodes or links from a road, railways, or power grid to disable the network. In the context of critical infrastructure protection, the set interdicted would be the set of assets most vulnerable to attack and in greatest need of protection.

A recent review of network vulnerability interdiction approaches (Grubestic et al. 2008, 90) points out that often, "network facilities are assigned importance to system operability prior to assessing the impacts of a disruption to justify the interdiction scenario examined." Grubestic and colleagues indicate that these priority rankings are based on "simple, graph theoretic measures". Since critical infrastructure systems have such a large set of components, interdiction analysis follows a similar two-step process as the multi-criteria methods we reviewed above. Interdiction analyses first identify important or critical facilities through some graph theoretic measures, and then apply vulnerability assessment to the identified nodes or arcs.

The review discusses two types of indicators of asset importance used in interdiction analysis, global graph theoretic measures, and local network measures. The global indicators summarize overall network structure and enable comparison of networks. They are based on nodes, links, and subgraphs.<sup>16</sup> For example, the Beta index,  $\beta = e/v$ , where  $e$  = the number of edges or links in the graph or network, and  $v$  = the number of vertices or nodes in the graph or network, is a simple index of complexity, which can identify whether the network involved has a treelike structure or a circuit network. On the other hand, local network measures are computed for individual links or nodes, and highlight their relative topological features. We have already encountered the simplest local measure of nodal accessibility in Lewis's network analysis, the degree of node. As discussed above, higher degree nodes are assumed to be more critical for system performance. Among other local indicators, the review identifies a local measure of accessibility,  $T$  obtained by powering network adjacency relationships  $C$ . "Each power  $n$  of  $C$  represents the number of nodal sequences of length  $n$  linking each pair of nodes." (93) This indicator can suggest how proximate a node is to other nodes within a system. The larger the value of  $T$ , the more accessible the node. Another indicator of nodal importance is the shortest path between node pairs. Here a smaller path indicates more accessible nodes.(Grubestic et al. 2008, 93-94). Also, recently, a new local network measure to assess network component importance has been proposed by Nagurney and Qiang (2008) which "captures demands, flows, costs and behavior on networks".

Vulnerability assessment in interdiction analyses, according to the review, can be of three types: scenario specific, strategy specific, or structured. A scenario specific study may focus on the impacts of disruptions to a transportation system due to a natural disaster, such as increases in shipment length and cost of transporting goods (Ham, Kim

---

<sup>16</sup> A subgraph is a subset of a graph, e.g., if a graph represents the regional road system, a subgraph could be a city's in the region road system.

and Boyce 2005). Strategy-specific approaches are characterized by specific node-arc attack strategies, and benefit from the work on scale-free and small world networks already discussed. These approaches simulate the removal of nodes or arcs in specific networks to determine the resulting connectivity of the network. Latora and Marchiori (2005) use this type of approach to assess the most critical nodes or arcs in a network. They test for the redundancy of an asset “by calculating the performance of a disturbed network and comparing it with the original one.” (Latora and Marchiori 2005, 015103-1) They found that the more highly connected nodes are not necessarily the most critical. Structured approaches utilize optimization modeling to identify best and worst-case interdiction scenarios. Structured modeling can be focused on several aspects of a network, e.g., network attributes, connectivity, flow or capacity (Grubestic et al. 2008, 95-100). For example, the recent work of Scaparra and Church (2008a,b) involves the development of optimization algorithms for supply systems “to minimize the cost of the or the weighted distance of supplying all demand, where each demand is assigned to its closest facility” . The objective of this research is to identify the subset of assets, which if fortified or hardened, provides the best protection against the worst case loss of the total number of non-fortified facilities. Structured approaches have also developed connectivity and flow optimization interdiction models. (Murray, Matisziw and Grubestic 2007). Optimization modeling typically requires extensive computation, and is opaque to stakeholders.

### **5.3.1 Strengths and weaknesses of the interdiction approach to prioritizing**

The network interdiction approach to prioritizing employs a larger set of indicators than Lewis, both global and local to test for priority. Among these indicators are indicators of connectivity and flow, path length, centrality and betweenness, some of which are more informative than degree of node if the connectivity or flow within a network is important. But such indicators may require real data on flow and performance, which may be difficult to obtain for critical infrastructures. In addition, this type of approach is more opaque to stakeholders, requiring greater mathematical training than other approaches we reviewed.

After reviewing the literature for approaches to interdiction theory, Grubestic et al. apply the various measures they identified in their review to the Abilene Internet system (a U.S. network of internet routers for research universities) for which they obtained empirical data. With respect to identifying critical nodes or arcs, their application revealed that: a) global indicators of importance may provide some insight into the type of system, but are not helpful in identifying critical nodes or arcs in a system; b) the degree of node indicator is not helpful when dealing with a sparse network such as the Abilene system, but other local indicators can be more useful, such as the  $T$  index of accessibility, which identified the four most critical nodes in the system; and c) even local indicators fail to capture the complexities of nodal importance. They argue that, “parity in a local approach can mask the criticality of nodes in a system, particularly with respect to flow and use” (109). Finally, the authors warn that the criticality of a node or arc cannot be evaluated in an *aspatial* way, without taking into account its location within

the network topology and the possibilities for movement between all other nodes or arcs that remain in the system after a hypothetical attack. (110)

## 5.5 Prioritizing Critical Infrastructure Assets and Systems Analysis

In this paper, we have reviewed two major multi-criteria approaches to prioritization of critical infrastructure assets, and two types of network analysis, Lewis's network analysis and interdiction theory. As discussed above, both multi-criteria approaches fail to address the infrastructure systems as systems, and their spatial nature. The strength of Lewis's network theory is its computational simplicity and low data requirements. Its application to scale-free networks is insightful, and the accompanying software that models the incapacitation of nodes, and the propagating impacts on a network is a useful tool to educate professionals on network characteristics and cascading failures. However, the approach, as we discussed, faces challenges. Even its application to the Internet, the very system that led Barabasi (2002) to formulate the concept of scale-free networks, has its critics. For example, Doyle and his colleagues (2005, 14501-502) have found that in the Internet, the hubs identified by the greatest degree of linkages are not necessarily the critical nodes. As they argue, systems like the Internet have characteristics that are not captured by network theory, such as protocols and multiple layers of feedback control. They conclude that scale-free network indicators "collapse when faced with real data or when examined by domain experts".

Networks are systems, but they are abstract systems, stripped down to two basic elements, nodes and links. Even the stock-flow diagrams of systems analysis provide more information, and a broader type of systems analysis<sup>17</sup> addresses aspects of a system that are not adequately reflected in either multi-criteria or network approaches. Further, systems analysis is more appropriate for determining the priority of assets in critical infrastructure systems, because determining the criticality of components fundamentally involves understanding the performance of a system. The approaches we reviewed are all concerned with performance, but only systems analysis diagrams aim at outlining how the vital components of a system achieve system performance.

In systems analysis, there are two major tools to model the performance of a complex system, stock and flow and causal loop diagrams. Although causal loop diagrams are more popularly identified with the systems approach, specifically systems dynamics, stock and flow diagrams can retain more information about the flow of a good through a system or the performance of a system. (de Rosnay 1979) For example, in a stock and flow diagram of New York City's water system or an oil transmission system, see Figure 4 below, sources that provide inputs, transmission conduits, valves (that control the volume of flows), reservoir or stock elements, and sinks that receive outputs can be identified. Information flows along the system can also be incorporated into such models. Retaining the information about the role that an asset plays in a system, and where the asset is located in a system is important to determine its criticality. In addition, a stock and flow diagram can depict redundancy or lack of redundancy in a system.

Stock and flow diagrams typically incorporate the capacity of the elements

---

<sup>17</sup> Such as, an emphasis on the environment of a system, or on performance standards for a system.



involved, but to be more useful for determining the criticality of a component of an infrastructure system, they could be augmented to incorporate the condition of the component, the availability, cost, and rapidity of replacement if disabled, and security measures at the asset level, as well as the protocols or regulations that control the system and component functioning. Hypertext or a simplified geographic information system can be used to add more functionality to the standard stock and flow diagram by enabling layering of information per component. Layered information would remain spatially embedded per component, and would facilitate identifying various aspects of resilience, including levels of robustness, redundancy, resources available in case of a component failure, as well as the rapidity of restoring component function. Prioritization of components could then be based on the resilience of system components, and the extent of flow or processing provided by the component. For example, old aqueduct segments in Upstate New York and old water mains running under Manhattan could both be in similar poor condition, but the old aqueduct segment would be likely prioritized because of its greater flow capacity and location in the system. However, if adequate reservoir conditions obtain near the city, and if the rapidity in which such an aqueduct segment can be repaired in upstate New York outweighs the magnitude of disruption, time delays and cost to repair a major water main break in mid-Manhattan, then the replacement of old water mains in mid-Manhattan could receive a higher priority. Of course, this systems approach to prioritization would involve much analytical work, including some ranking of resiliency criteria. However, the analytical work would be useful for system maintenance, traditional resource allocation, as well as critical infrastructure protection. Further, the basic stock and flow diagram is a simple conceptual model which can be useful in making decisions that involve multiple stakeholders. It provides a handy mental model that incorporates more system-specific information than network models.

In addition, systems models can be interlinked to indicate interdependence. A national effort to model the nation's critical infrastructure interdependencies has already been launched (Min et al. 2007) and the researchers at the national labs leading the effort are using a combination of system dynamics causal feedback loop and Integrated Definition Methods (IDEF) diagrams to model system interdependencies.

## **6. Conclusion**

Recent national policies and plans mandate the protection of critical infrastructure systems. The mandate to protect is interpreted as the need to make less vulnerable or more resilient the vital systems on which we all depend. Resource constraints and the vastness of these systems, which are often comprise thousands of assets or components, challenge the traditional resource allocation methods employed by public finance to prioritize projects. Traditional economic evaluation methods, such as cost-benefit or cost-effectiveness methods, are only appropriate after system assets or components have been prioritized and narrowed down to a few. Multi-criteria approaches to prioritization have been adapted to apply to critical infrastructure systems. But these approaches fail to appropriately capture the systemic and network characteristics of such systems. While Lewis's network theory and interdiction network analyses are important tools which can capture important network characteristics of critical infrastructure components, they also

face challenges and limitations. To address some of these challenges, this paper proposes the use of systems analysis, in particular, the use of enhanced stock and flow diagrams which could retain the network attributes of a system, and yet provide more information on the function of components in such systems. Such an approach would also have the capacity to indicate interdependencies among systems.

## References

- Anderson, Christopher W., Kash Barker and Yacov Y. Haimes. 2008. Assessing and Prioritizing Critical Assets for the United States Army with a Modified RFRM Methodology. *Journal of Homeland Security and Emergency Management*. 5(1) web page.
- Aronson, J. Richard and Eli Schwartz. 2004. Chapter 6. Cost-benefit analysis and the capital budget. In *Management Policies in Local Government Finance*. Editors, J. Richard Aronson and Eli Schwartz. Washington, D. C.: ICMA Press.
- Barabasi, A.-L. 2003. *Linked: How Everything is Connected to Everything Else and What it Means for Business, Science, and Everyday Life*. PLUME Cambridge, MA
- Calia, Roland. 2001. Priority-setting Models for Public Budgeting. Government Finance Officers Association
- De Rosnay, Joel. 1979. *The Macroscope*. New York: Harper and Row. Accessible at: <http://pespmc1.vub.ac.be/MACRBOOK.html>
- Doyle, J. C., D.L. Anderson, L. Li, S. Low, M. Roughan, S. Shalunov, R. Tanaka, and W. Willinger. 2005. The “robust yet fragile” nature of the Internet. *Proceedings of the National Academy of Sciences*. <http://www.pnas.org/cgi/doi/10.1073/pnas.0501426102>.
- Granovetter, Mark. 1973. The Strength of Weak Ties. *American Journal of Sociology*, 78(6), 1360-1380 (1973).
- Grubestic, Tony H., Timothy C. Matisziw, Alan T. Murray, and Diane Snediker. 2008. Comparative Approaches for Assessing Network Vulnerability. *International Regional Science Review*. 31(1) 88-112.
- Haimes, Y.Y. 2004. *Risk Modeling, Assessment, and Management*. 2nd Edition. Hoboken, New Jersey: Wiley.
- Haimes, Y.Y. 2006. On the Definition of Vulnerabilities in Measuring Risks to Infrastructures. *Risk Analysis*, 26(2): 293-296.
- Haimes, Y.Y., S. Kaplan, and J.H. Lambert. 2002a. Risk filtering, ranking, and management framework using hierarchical holographic modeling. *Risk Analysis*. 22(2): 381-395.
- Haimes, Y.Y., T.A. Longstaff, and G.A. Lamm. 2002b. Balancing Promise and

Risk with Information Assurance in Joint Vision 2020. *Military Operations Research*. 7(3): 31-46.

International Panel on Climate Change (IPCC). 2007. *Climate Change 2007- Impacts Adaptation and Vulnerability*. Contribution of Working Group II to the Fourth Assessment Report of the IPCC.

IPCC. 2001. *Climate Change 2001. Overview of Impacts, Adaptation, and Vulnerability to Climate Change*. Working Group II Contribution to the Third Assessment Report of the International Panel on Climate Change.

Kaplan, R.S. and D.P. Norton. 1992. The Balanced Scorecard – Measures that Drive Performance. *Harvard Business Review*, Jan./Feb.: 71-79.

Latora, Vito, and Massimo Marchiori. 2005. Vulnerability and protection of infrastructure networks. *Physical Review E* 71, 015103-1-4.

Leung, M., J.H. Lambert, and A. Mosenthal. 2004. A Risk-Based Approach to Setting Priorities in Protecting Bridges Against Terrorist Attacks. *Risk Analysis*, 24(4): 963-984.

Lewis, Ted. 2006. *Critical Infrastructures Protection in Homeland Security*. Hoboken, NJ: Wiley and Sons

Lowrance, W.W. 1976. *Of Acceptable Risk: Science and Determination of Safety*. Los Altos, CA: William Kaufman, Inc.

Milgram, S. 1967. The small world problem. *Psychology today* 2, 60-67.

Millar, Annie. 1988. Selecting Capital Investment Projects for Local Governments. *Public Budgeting and Finance*. Autumn 1988, p. 63-77.

Min, Hyeung-Sik J., Walter Beyeler, Theresa Brown, Young Jun Son, and Albert T. Jones. 2007. Toward modeling and simulation of critical national infrastructure interdependencies. *IIE Transactions* 39, 57-71.

Mullen, Penelope M. 2004. Quantifying priorities in healthcare: transparency or illusion? *Health Services Management Research*. February 2004, 17(1): 47-58.

Mullen, Penelope M. and P. Spurgeon. 2000. *Priority Setting and the Public*. Oxon: Radcliffe Medical Press, 2000.

Murray, A.T., T.C. Matisziw, and T.H. Grubestic. 2007. Critical network infrastructure analysis: Interdiction and system flow. *Journal of Geographical Systems* 9: 103-117.

Nagourney, Anna and Qiang Qiang. 2008. A network efficiency measure with application to critical infrastructure networks. *Journal of Global Optimization*. 40:261-275.

National Oceanic and Atmospheric Administration (NOAA) Coastal Services Center, Community Vulnerability Assessment Tool.

<http://www.csc.noaa.gov/products/nchaz/htm/tut.htm>

National Research Council. 2002. *Making the Nation Safer*. National Research Council.

Office of the President. 2002. *The National Strategy for Homeland Security*, July 2002.

Office of the President. 2003. The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets. February, 2003.

Office of the President. 2003. Homeland Security Presidential Directive (HSPD-7) December 17, 2003.

<http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html>

Perrow, Charles. 1984. *Normal Accidents*. New York: Basic Books.

President's Commission on Critical Infrastructure Protection (PCCIP). 1997. *Critical Foundations: Protecting America's Infrastructures. The Report of the President's Commission on Critical Infrastructure Protection*. Washington D.C.

<http://handle.dtic.mil/100.2/ADA331523>

Rinaldi, Steven M., James P. Peerenboom, and Terrence K. Kelly. 2001. Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies. *IEEE Control Systems Magazine*. Pp. 11-25. December 2001.

Scaparra, Maria and Richard L. Church. 2008a. A bi-level mixed-integer program for critical infrastructure protection planning. *Computers and Operations Research* 35: 1905-1923.

Scaparra, Maria and Richard L. Church. 2008. An exact solution approach for the interdiction median problem with fortification. *European Journal of Operational Research*. 189: 76-92.

Science Applications International Corporation (SAIC). 2002. *A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection*. Prepared for The American Association of State Highway and Transportation Officials' Security Task Force. May 2002. Vienna, VA.

Stokey, Edith and Richard Seckhouser. 1978. *A Primer for Policy Analysis*. NY: W.W. Norton and Co.

Tierney, Kathleen and Michel Bruneau. 2007. Conceptualizing and Measuring Resilience. A Key to Disaster Loss Reduction. *TR News*. May-June 2007. 250:14-17.

U.S. Department of Homeland Security. 2006. *National Infrastructure Protection Plan*.  
[http://www.dhs.gov/xprevprot/programs/editorial\\_0827.shtm#1](http://www.dhs.gov/xprevprot/programs/editorial_0827.shtm#1)

U.S. Department of Homeland Security and US Environmental Protection Agency. 2007.  
*Water. Critical Infrastructure and Key Resources. Sector-Specific Plan as Input to the  
National Infrastructure Protection Plan*. May 2007. Accessed at  
[http://www.michigan.gov/documents/deq/deq-wb-wws-Water\\_SSP\\_5\\_21\\_230463\\_7.pdf](http://www.michigan.gov/documents/deq/deq-wb-wws-Water_SSP_5_21_230463_7.pdf)

U.S. Department of Homeland Security, Transportation Security Administration. 2007.  
*Transportation.. Critical Infrastructure and Key Resources. Sector-Specific Plan as Input  
to the National Infrastructure Protection Plan*. May 2007. Accessed at  
<http://www.dhs.gov/xlibrary/assets/nipp-ssp-transportation.pdf>

U.S. Department of Transportation, Research and Innovative Technology Administration,  
Bureau of Transportation Statistics. Press release, March 13, 2008. December 2007  
Airline Traffic Data. Found at:  
[http://www.bts.gov/press\\_releases/2008/bts013\\_08/html/bts013\\_08.html](http://www.bts.gov/press_releases/2008/bts013_08/html/bts013_08.html)

U.S. Patriot Act of 2001. Section 1016 Critical Infrastructure Protection Act of 2001,  
section (e)

Vogt, John A. 2004. *Capital Budgeting and Finance: A Guide for Local Governments*.  
Chapter 4. Prioritizing Capital Projects pp. 89-118. ICMA

Watts, D. 1999. Networks, Dynamics, and the Small-World Phenomenon. *American  
Journal of Sociology*. 105(2): 493-527. Sept. 1999.

Watts, D. and S.H. Strogatz. 1998. Collective Dynamics of 'small world' networks.  
*Nature*. 393:440-42





## Strategic Homeland Infrastructure Risk Assessment

---

The Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) produces the annual Strategic Homeland Infrastructure Risk Assessment (SHIRA) to provide decision makers within the infrastructure protection community with a comparative assessment of the risks to the Nation’s critical infrastructure and key resource (CI/KR) sectors from international terrorists and their affiliates. The report, designed to inform risk management decision making, builds upon a yearlong development process involving representatives from the Intelligence Community (IC) and the Sector-Specific Agencies (SSAs) identified by Homeland Security Presidential Directive 7 to represent the interests of each of the 17 CI/KR sectors in the Federal inter-agency community.

### The Process

To facilitate its assessment of risk to the Nation’s CI/KR sectors, HITRAC developed a process designed to evaluate the threat to, and vulnerability from specified terrorist attack methods, and the resulting consequences should the terrorist attack succeed.

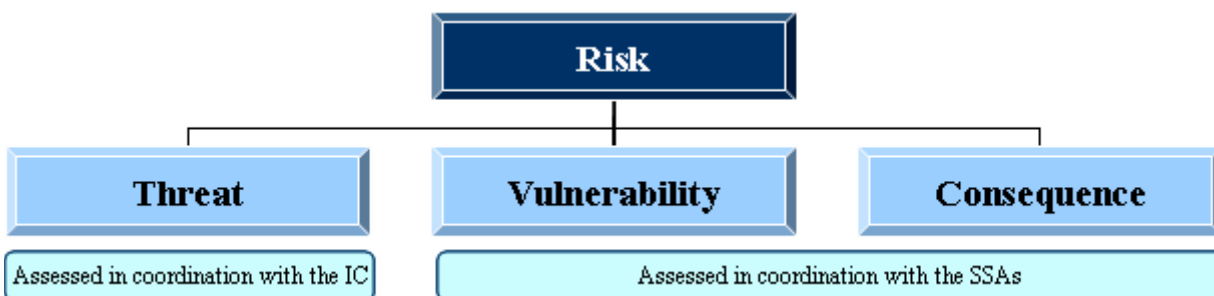


Figure 1: Assessed components of risk.

The process begins with identifying the attack methods of greatest concern to the IC, DHS, and the SSAs. HITRAC then works with the IC to assess the threat posed by each of the identified attack methods, based upon terrorist capability and intent to use the attack method against the Nation’s CI/KR. Concurrently, HITRAC works with the SSAs to create a separate scenario for each attack method applicable to the sector. The SSAs then rank the sector’s vulnerabilities to each of the attack methods relevant to the sector, and the likely consequences should the attack succeed, including loss of life, economic costs, and psychological impact. Finally, HITRAC combines the assessments of threat, vulnerability, and consequence into an overarching assessment of the terrorist risks to each sector, and the Nation.

---





**Threat-Based Approach to Risk**  
**Case Study: The Strategic Homeland Infrastructure Risk Assessment (SHIRA)**

**Geoffrey S. French**  
**Jin Kim**  
**Pasha Vasilev**  
**CENTRA Technology, Inc.**  
**4121 Wilson Blvd, Suite 800**  
**Arlington, VA 22203**  
**frenchg@centratechnology.com**  
**kimj@centratechnology.com**  
**vasilevp@centratechnology.com**

## Introduction

The culture of risk management is beginning to grow at the Department of Homeland Security (DHS). Created in response to the attacks of September 2001, the Department has as one of its primary missions to protect the nation from terrorism.<sup>1</sup> Five years after its creation, and through several reorganizations, DHS still struggles to master risk management with respect to terrorism. Although DHS realized the need for the collaboration of intelligence and security professionals to jointly assess risk at its inception,<sup>2</sup> it was not until the formation of the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) that DHS had a truly integrated approach to terrorism risk analysis.

Risk, defined in the National Infrastructure Protection Plan (NIPP) as a “measure of potential harm that encompasses threat, vulnerability, and consequence,”<sup>3</sup> guides the DHS infrastructure protection community in its analyses and assessments to better inform decision-making. Although the NIPP also includes natural disasters or other incidents in its definition of risk,<sup>4</sup> this paper will focus on terrorism risk, describing the organizational development and convergence of DHS’ intelligence and infrastructure protection areas – changes designed to bring forth a cultural change of collaboration. In addition, the paper will identify current problems and hurdles with regard to a terrorism risk culture. The case study will focus on a successful current threat based approach to risk, the Strategic Homeland Infrastructure Risk Assessment (SHIRA). Finally, this paper will propose a path forward in leveraging the success of the SHIRA to better meet the needs of terrorism risk analysis and assessments that inform strategic planning to enhance the protection and preparedness of the nation’s CIKR.

### Recognizing the Need for a Threat-Based Strategy

CIKR is at the heart of the nation’s economy and way of life. From the Banking and Finance Sector to the Food and Agriculture Sector, the 18 CIKR sectors form the backbone of the United States.<sup>5</sup> The preponderance of CIKR in the United States is owned privately, making the federal government’s duties with respect to its protection challenging. Homeland Security Presidential Directive 7 (HSPD-7) established the need

---

<sup>1</sup> DHS website, <http://www.dhs.gov/xabout/strategicplan/index.shtm>, accessed 10 April 2008.

<sup>2</sup> *Homeland Security Act 2002*, <http://www.whitehouse.gov/deptofhomeland/bill/>, accessed 11 April 2008.

<sup>3</sup> *National Infrastructure Protection Plan*. Department of Homeland Security, 2006, 105, [http://www.dhs.gov/xprevprot/programs/editorial\\_0827.shtm](http://www.dhs.gov/xprevprot/programs/editorial_0827.shtm), accessed 11 April 2008.

<sup>4</sup> *Ibid.*

<sup>5</sup> The eighteen CIKR sectors are: Agriculture and Food, Banking and Finance, Chemical, Commercial Facilities, Communications, Critical Manufacturing, Dams, Defense Industrial Base, Emergency Services, Energy: Electric, Energy: Oil and Gas, Government Facilities, Information Technology, Monuments and Icons, Commercial Nuclear Reactors, Materials, and Waste, Postal and Shipping, Public Health and Healthcare, Transportation: Aviation, Transportation: Highways, Transportation: Maritime, Transportation: Mass Transit, Transportation: Pipelines, Transportation: Rail (Freight), Water: Drinking Water, Water: Wastewater.

to create roles and responsibilities “for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks.”<sup>6</sup> The NIPP, developed by the Office of Infrastructure Protection, outlines the overarching structure to blend together current infrastructure protection programs with future requirements under a single program.<sup>7</sup>

This blending requires a strategic risk analysis that informs the prioritization of federal government resources for CIKR protection. Risk, a function of the likelihood of an unwanted event and its impact or effects, translates into a function of threat, vulnerability, and consequences in terrorism risk analysis; threat and vulnerability constitute the likelihood.<sup>8</sup> There are many techniques and approaches to the risk calculus; but at the core of sound risk analysis are the requirements that it be: objective, transparent, repeatable, accurate, and discriminating. Because risk models come in various forms (quantitative, semi-quantitative, and qualitative) there are competing ideas for what constitutes an effective risk model. Quantitative proponents may argue a strict adherence to probability theory; however, in situations where data are sparse – as is with intelligence and infrastructure – the precision that quantitative models should deliver is artificial. Strategic risk analysis for CIKR dictates a logic-based or semi-quantified approach. Using sound logic, fully addressing the core requirements of risk analysis, and focusing on the problem should be the tenets for strategic risk analysis.

Threat analysis is an essential factor of strategic planning. Although this appears to be self evident, some security analysis models do attempt to assess risk without assessing threat. Models that lack a threat component appeal to users who assume that the government has a monopoly on threat information and that they have no way of obtaining it from the government. The CARVER methodology, one of the best-known examples of an analytic tool that does not have a threat component, allows a user to prioritize attack scenarios by focusing exclusively on vulnerability and consequence.<sup>9</sup> Although there are significant challenges in public-private information sharing, this solution—to simply ignore threat—is misleading at best and disingenuous at worst. It overstates unlikely scenarios, especially attacks where the adversary has a very low capability.<sup>10</sup> This can cause an organization to overlook scenarios that are much more likely, even though they do not produce catastrophic consequences. Security and risk analysis without threat is a two-legged stool; because it may lead to illogical conclusions, it may be a poor foundation for any serious prioritization of efforts or resources.

Even simplistic threat assessments allow some meaningful differentiation of threat levels. The Federal Emergency Management Agency guide on risk assessment (FEMA 452), for

---

<sup>6</sup> *Homeland Security Presidential Directive 7*, December 17, 2003, <http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html>, accessed 10 April 2008.

<sup>7</sup> *National Infrastructure Protection Plan*, 1.

<sup>8</sup> *National Infrastructure Protection Plan*, 35.

<sup>9</sup> See the Product Surety Center’s primer, “CARVER Plus Shock Method for Food Sector Vulnerability Assessments,” 2005.

<sup>10</sup> For an in-depth discussion of the repercussions of ignoring terrorist threat, see Jeremy Shapiro’s “Managing Homeland Security,” The Brookings Institution: Washington DC, 2008. [http://www.brookings.edu/papers/2007/0228terrorism\\_shapiro\\_Opp08.aspx](http://www.brookings.edu/papers/2007/0228terrorism_shapiro_Opp08.aspx), accessed 10 April 2008.

example, allows a user to make an estimation of threat based on the complexity of the task and the difficulty of obtaining and working with the necessary materials.<sup>11</sup> Although this has the potential to underestimate the capability of a terrorist group in an attack method that they have not demonstrated, it does allow an analyst to review open-source information and prioritize the threat accordingly.

This type of model would suffice for an individual organization assembling a risk-based strategy for its own security efforts. However, it does not allow a comparison of risk levels across organizations, given the potential for differences of opinion in threat levels. For equitable comparison, there needs to be a central authority to coordinate and – at a minimum – set the assumptions for the threat analysis. For a national-level comparison of infrastructure, it falls upon DHS to provide that threat analysis.

For CIKR risk, there are two major communities – the Intelligence Community (IC) and the infrastructure protection community – that must collaborate on all aspects of risk to produce the most accurate assessments for terrorism risk to critical infrastructure. Similar to the military decision-making process where intelligence initiates the planning, and all functional areas participate in the entire process, CIKR risk assessments must be shepherded by the infrastructure protection community with threat as the initiating component. The *threat* referred to in the NIPP is an intelligence-based estimate on terrorism – the unwanted act or event in the risk equation.<sup>12</sup> A threat-based strategy, however, means that all components of risk (threat, vulnerability, and consequence) model are shaped by the focus on terrorism. According to Jeremy Shapiro of the Brookings Institute, “[T]his analysis of the terrorist threat implies several priorities for U.S. homeland security—and, conversely, several areas that do *not* need greater attention or spending.”<sup>13</sup> A threat-based approach to terrorism risk shapes the decision-making environment for the policy-maker.

### *Threat*

Threat, defined for CIKR risk purposes as an intelligence-based estimate of terrorism against critical infrastructure, must incorporate the evidence along with the analysis of subject matter experts on terrorist capabilities and intentions to attack the United States. This estimate must reflect the judgment of the level of government to which the threat and risk analyses apply. For example, an intelligence-based estimate for a strategic level risk assessment model may not be applicable for an assessment for tactical purposes. Although the information sharing at DHS is evolving to a more effective system, inclusive of state and local governments as well as federal, the nature of intelligence and protection of sources and methods makes the prospects of a strategic level assessment fully being applicable at a tactical level unlikely. However, the prospects bode well for sharing of knowledge and understanding of the estimates between the levels of government.

---

<sup>11</sup> Federal Emergency Management Agency, FEMA 452. Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings, January 2005, p 1-21.

<sup>12</sup> *National Infrastructure Protection Plan*, 39.

<sup>13</sup> Shapiro.

Intelligence is not an exact science; therefore, DHS should not try and make it such by attempting to force a highly quantified model for the sake of an equation. Rather, one must tailor the model to the assessment process and allow review of the data (as appropriate and in accordance with classification standards) and analyses behind the threat assessment for debate. This transparency will in turn allow alternative analyses and assessments to build upon the overall risk analysis. Additionally, the threat methodology must represent the community of stakeholders. In developing a threat model that incorporates the collective knowledge and data from the IC, along with the security needs of the infrastructure protection community, the model must serve as a mechanism to consider multiple theories, weigh evidence, and guide consensus.

### *Vulnerability*

In the context of terrorism risk, developing a methodology for vulnerability analysis must take into account the potential adversary. Therefore, a design of the vulnerability model should incorporate terrorism experts who can provide the insight through the lens of the terrorists. Models that do not utilize terrorism expertise in the development have the potential to bias the model towards unrealistic expectations that may create unattainable standards of invulnerability.<sup>14</sup> Risk analyses support the allocation of limited resources; a vulnerability model that only considers the judgments of security experts misses the vector analysis that terrorism experts can bring. For example, many vulnerability models are only developed with experts that look at the problem of how security professionals view the vulnerabilities and not how adversaries view the vulnerabilities. Collaboration between security experts and terrorism analysts provides the ideal approach to developing a vulnerability model for terrorism risk.

### *Consequence*

As defined in the NIPP, a consequence assessment should measure the potential loss in four categories: public health and safety, economic, psychological, and governance impacts.<sup>15</sup> The four categories are consistent with the ideology and motivations of the terrorist threat – terrorist goals to destroy the U.S. economy, government, and impose psychological harm. In practice, however, most methodologies focus on economic and loss of life because those aspects are more easily quantified. Quantification of the economic losses and loss of life is an important aspect of modeling consequence, but that alone diverts focus from the whole which includes public health and safety, psychological, and governance impacts. Some methodologies measure economic loss and loss of life quantitatively with actual dollar values and relegate the other categories spelled out in the NIPP to qualitative assessments that are not integrated, leaving the assessment bereft of fundamental elements crucial to support decision-making at the national level of government. Therefore, whatever the type of methodology (quantitative, semi-quantitative, or qualitative), it must incorporate all categories into its methodology. Quantification is not merely using real dollar values; therefore, one would have to

---

<sup>14</sup> Shapiro.

<sup>15</sup> *National Infrastructure Protection Plan*, 103.

establish equivalencies or utilities to develop consequence models quantitatively that take into account all categories where the measurements do not directly translate into dollar values. In this approach, a risk index or levels of severity are appropriate for risk analysis.

### *Wrapping Our Hands Around Threat*

The infrastructure protection community can do all it can to create a collaborative environment between all levels of government and the private sector; however, the challenges with respect to obtaining threat assessments for risk purposes are uniquely a government-to-government function. “To receive better threat information from the U.S. government, the critical infrastructure protection community must acknowledge inherent limitations of intelligence analysis and then help formulate requests for threat information, knowing that no single approach or tool will give a decision-maker the full perspective needed to manage risk.”<sup>16</sup> DHS is the unique government organization that makes this government-to-government interaction a reality. Through DHS, the IC and infrastructure protection community can learn each others’ characteristics and develop a common understanding of the requirements for a terrorism risk assessment.

### **Case Study – Strategic Homeland Infrastructure Risk Assessment**

The Strategic Homeland Infrastructure Risk Assessment (SHIRA) provides a national-level terrorism risk assessment that offers a snapshot of the highest risk to the nation’s critical infrastructure and key resources. The SHIRA utilizes an interagency, DHS-led process to analyze and produce assessments of threat, vulnerability, and consequence, and combines the data into a single measurement of risk for purposes of comparison. The methodology uses a structured method to quantify government and non-government expert opinions. Where modeling or quantified assessments already exist, their output can be easily captured in the SHIRA framework, which is based on accepted risk analysis principles and was designed to be as simple as possible. Text descriptions used by government experts to assign numerical values were designed to best match the data quality and to minimize double-counting of risk factors.

The SHIRA is a scenario-based model where Sector Specific Agencies (SSAs) that represent each CIKR sector applied terrorist attack methods of concern to their individual sectors. HITRAC, through coordination with the IC partners, provides a standard set of terrorist attack methods and descriptions. The SSAs then apply selected attack methods of concern to their sectors and create worst, most-likely scenarios. The IC assesses the threat of each attack method to each sector and the SSAs assess the vulnerability and consequence for each of their respective scenarios. Where applicable, HITRAC will assess vulnerability and consequence through independent outside subject matter experts to assist and augment the SSAs in their rankings.

---

<sup>16</sup> French, Geoffrey S. “Intelligence Analysis for Strategic Risk Assessments”. *Critical Infrastructure Protection: Elements of Risk*. Critical Infrastructure Protection Program: George Mason University School of Law, December 2007, 12. [http://cipp.gmu.edu/archive/RiskMonograph\\_1207\\_r.pdf](http://cipp.gmu.edu/archive/RiskMonograph_1207_r.pdf), accessed 15 April 2008.

The relationship between the threat, vulnerability, and consequence assessments is represented:

$$\mathbf{Risk} = \mathbf{Threat} \times \mathbf{Vulnerability} \times \mathbf{Consequence} \text{ (Equation 1)}$$

The risk is computed based on a standard probabilistic model where a quantification of a consequence is weighted in proportion to the probability that it will occur. This is expressed:

$$\mathbf{R} = \mathbf{P} \times \mathbf{C} \text{ (Equation 2)}$$

where **R** is risk, a measure of the concern presented by a threat scenario, **P** is the probability that the threat scenario will occur, and **C** is the consequence if the threat scenario occurred and an attack was successful.

It is important to note that the number of terrorist attacks does not support a statistically significant calculation of probability. The SHIRA assesses the severity of threat and vulnerability as a proxy for probability. The probability that a threat scenario will occur is therefore calculated in terms of the likelihood that an adversary will launch the attack described in the attack method (represented by the variable **T<sub>P</sub>**, where the subscript is used to note probability), and the likelihood that the target of the threat scenario is vulnerable to the attack (variable **V<sub>P</sub>**). This is expressed:

$$\mathbf{P} = \mathbf{T}_P \times \mathbf{V}_P \text{ (Equation 3)}$$

Thus, the risk equation becomes:

$$\mathbf{R} = (\mathbf{T}_P \times \mathbf{V}_P) \times \mathbf{C} \text{ (Equation 4)}$$

## **SHIRA Threat**

DHS works closely with the other members of the IC to identify the appropriate terrorist attack methods and then quantify the threat from each. The attack methods used in the SHIRA are those where terrorists have demonstrated a capability or where intelligence reporting indicates that terrorists are making an effort to acquire the capability.

The SHIRA threat analysis addresses both a terrorist group's capability and intent to attack. To estimate capability, DHS examines both the demonstrated capability and takes into account the group's efforts to acquire or augment that capability. To estimate intent to attack, DHS first assesses general terrorist interest in attacking the sectors of infrastructure and then examines specific intent to use one of the attack methods against a specific sector. These are illustrated in Figure 1 and explained in more detail below. The benefit of this approach is that it is relatively simple (compared with other approaches to

probabilistic threat), it measures severity of threat in a way that allows expert consensus, and the results closely match qualitative threat analysis.

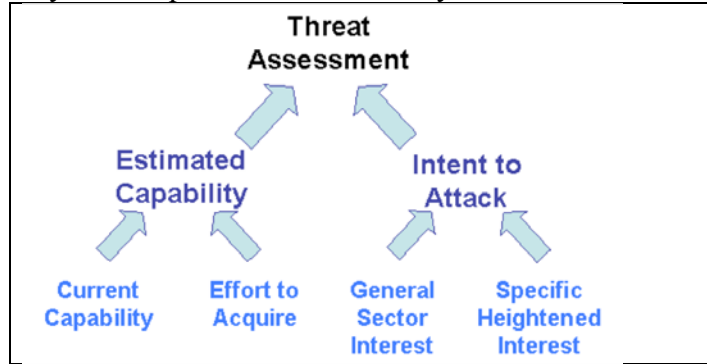


Figure 1: Components of Threat in the SHIRA Model

### *Framework for the Analytic Process*

The SHIRA approach supports interagency consensus on the analytic conclusions in three ways. First, DHS uses defined thresholds to delineate stages of capability and degrees of intent. Second, DHS provides ranking guidance to help participating analysts assess operational capability (i.e., the means, materials, and expertise to launch the attack described in the attack method), operational plans (i.e., a terrorist initiative to which personnel or funding has been assigned), and other relevant factors in a consistent manner. Third, DHS provides the initial rankings and the intelligence reporting that contributed to the analytic judgments. This approach provides transparency into the process and rankings, which allows debate and a means for resolution.

### *Estimated Capability*

When assessing terrorist capabilities, DHS uses analysis of both historical attacks and intelligence reporting for an assessment of near-term risk. The SHIRA defines estimated capability as having two components: current capability and effort to acquire the capability. *Current capability* considers historical incidents and knowledge of existing capability, whereas *effort to acquire* evaluates an adversary's attempts to gain or build upon a capability (the maturity of the acquisition process or the degree of effort and progress of the acquisition process). For a high-level assessment such as the SHIRA, an assessment of the effort to acquire a capability helps account for uncertainty, as well as provides a mechanism for allowing for the potential increase in capability within the near-term timeframe of the analysis.

Table 1 lists the ranking levels and criteria for the components of estimated capability. The criteria for *effort to acquire* are meant to represent an intermediate step to the next level of *current capability*. (That is, a ranking of 3 in effort to acquire is intermediate between level 2 and 3 in current capability.) In this way, the ranking table would be used as a progression from level 0 in effort to acquire to a 4 in current capability.



Component	Ranking level				
	0	1	2	3	4
<b>Effort to Acquire a Capability</b>	No effort to acquire the capability	Adversary is pursuing the capability by attempting to develop internal expertise, obtain materials, or recruit experts	Adversary has an organized attempt to obtain either materials or expertise needed to advance the capability	Adversary has internal training, expertise, and access to materials required to develop the capability	Adversary has training or operational plans to develop the capability to launch an attack in the United States
<b>Current Capability</b>	No evidence of existing capability to execute the attack	Evidence of existing pre-operational skills	Suspected operational capability	Overseas operational capability confirmed by credible intelligence	Domestic operational capability confirmed by credible intelligence

*Intent to Attack*

As stated above, to estimate intent to attack, DHS first assesses the terrorist group’s general interest in attacking a sector of infrastructure and then examines specific intent to use one of the attack methods against a specific sector. *General sector interest* reflects the adversaries’ general desire to attack a specific sector, irrespective of attack method. As with its approach for estimating capability, DHS defines criteria for separating the sectors into tiers. The criteria are meant to be specific enough to make clear distinctions between the tiers, but flexible enough to accommodate analytic judgments. The tiers do not reflect raw numbers of reports, but rather the meaning of the reports. Table 2 contains the definitions for the tiers for general sector interest.

Ranking	Description
Tier 1	There is a body of evidence or credible reporting and analysis including multiple threat or threat streams originating from numerous sources regarding the intent of the group being evaluated to attack the sector in the United States.
Tier 2	There is credible reporting and analysis depicting a threat originating from a single source or a limited set of sources regarding the intent of the group being evaluated to attack the sector in the United States
Tier 3	There is reporting depicting threat or threat streams originating from sources of undetermined credibility regarding the intent of the group being evaluated to attack the sector in the United States.
Tier 4	There is no known information or analysis concerning a terrorist threat to the sector in the United States.

The ranking of *general sector interest* is used as the baseline of a terrorist intent to attack the sector in ranking scenarios (i.e., the use of a specific attack method against a specific sector) where there is no intelligence to identify the intent of a terrorist group to attack. Where scenario-specific intelligence is available, DHS assesses *specific heightened interest*, which reflects historical precedent or current intelligence reporting. Although foreign attacks provide many of the data with regard to intent, the SHIRA criteria

separate those that occur in security environments different from the United States. Table 3 defines the rankings used for specific heightened interest in a scenario.

Ranking	Description
A	Intelligence indicates a <b>heightened interest</b> in using the attack method against the sector in the United States or Western Europe (e.g., operational plan or attack, or credible source, multiple reports, sustained interest, etc.).
B	Intelligence indicates a <b>moderate interest</b> in using the attack method against the sector in the United States or Western Europe (e.g., multiple reports from different sources of varying credibility, recurring interest, etc.).
C	Intelligence indicates a <b>weak interest</b> in using the attack method against the sector in the United States or Western Europe (e.g., few reports of less than credible sources, anecdotal interest, etc.).
D	Any group has had a successful attack, failed attack, or disrupted operational plan to launch an attack against the sector outside of the <b>United States or Western Europe</b> using the attack method described.

*Combining the Estimates*

There are two ways of combining the intent and capability levels, depending on the needs of the overall risk model. The SHIRA model requires the quantification of the threat to support its risk analysis. This approach uses a measurement of severity as a proxy for probability, and each capability and intent levels are assigned a value between 0 and 1. By using a consistent logic to adjust the intervals between the values, the scale reflects analytic judgments of distance between the levels and translates the ordinal rankings into a cardinal value. Because the SHIRA model treats the two aspects of threat separately, it treats *estimated capability* and *intent to attack* as independent probabilities. The threat, therefore, is a function of (or the multiplication of) the capability and the intent to attack. The product is a value on a scale of 0 to 1.0 and used as the threat ranking in the SHIRA equation, treated equally with vulnerability and consequence. For risk models that do not allow multiplication or cannot utilize a quantified threat level, the SHIRA threat model can combine the two factors with Boolean logic and produce a threat level on a low to high scale, as appropriate (see Figure 2).

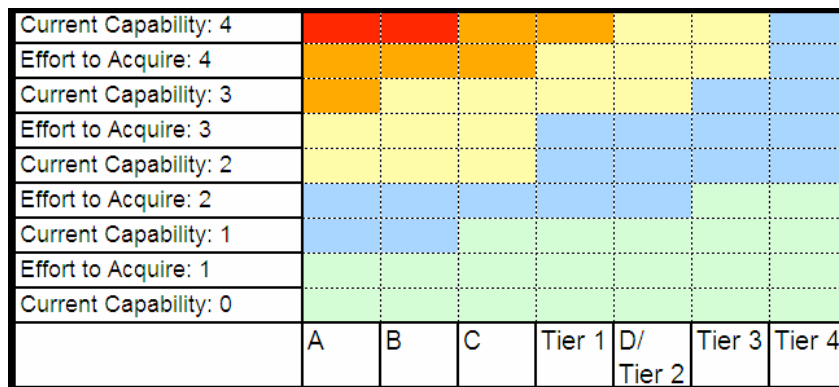


Figure 2: An illustration of Boolean combination of intent and capability levels where red indicates high, orange indicates medium-high, yellow indicates medium, blue indicates medium-low, and green indicates low.

The equation for  $T_P$  is:

$$T_P = (I \times Ca) \text{ (Equation 5)}$$

The final number provides an indication of the relative severity of the threat for each attack scenario and represents a probability that an attack will occur.

## **SHIRA Vulnerability and Consequence**

DHS works closely with the infrastructure protection community, through the NIPP framework, to obtain data and analytic judgments on vulnerability and consequence. SSAs, representing a unique community of interest within infrastructure, provide the expert judgments for their respective sector. Each sector utilizes the intelligence-based terrorist attack methods to create relevant scenarios for their sector under the guidance of worst-most likely; the SSAs apply an attack method to an asset, representative asset, or system in their sector that represent the worst-most likely scenario. For each scenario, a vulnerability and consequence rankings are determined through the SHIRA model framework.

### *Framework for the Analytic Process*

Similar to the process for the threat assessment, the vulnerability and consequence assessments follow the steps of defining thresholds and providing ranking guidance. DHS works with representatives from the SSAs who determine which attack methods pose nationally significant risk in their respective sectors and assess the consequences of and vulnerability to those potential terrorist attacks.

### *Vulnerability*

The SSAs take into account three different aspects of vulnerability: (1) the difficulty in identifying the asset and its criticality; (2) the effectiveness of the countermeasures in place in preventing the attack from succeeding; and (3) if the countermeasures fail, whether the attack will have the desired effect. This last consideration allows the SSAs to evaluate the robustness or the degree to which a CI/KR system can resist the attack. In many infrastructure systems, individual nodes may be highly vulnerable, but the system is still highly resistant to the destruction or disruption of a single node. As with the other risk factors, the SHIRA process provides the definitions and guidance for ranking each component of vulnerability.

<b>Component</b>	<b>Ranking Level</b>				
	<b>0</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>
<b>Recognizability</b>	Asset is very unlikely to be recognized; adversary would require a highly trained expert or access to classified or highly sensitive information	Asset is unlikely to be recognized; an adversary would require some special knowledge or training	Asset is somewhat likely to be recognized; an adversary would require a moderate amount of research	Asset is likely to be recognized; an adversary could identify this asset with minimal effort.	Asset is very likely to be recognized; any adversary could easily identify this asset.
<b>Countermeasure Effectiveness</b>	The existing countermeasures are very likely to defeat the attack.	The existing countermeasures are likely to defeat the attack.	The existing countermeasures are somewhat likely to defeat the attack.	The existing countermeasures are unlikely to defeat the attack.	The existing countermeasures are very unlikely to defeat the attack.
<b>Robustness / Resistance</b>	The asset is very likely to resist, withstand, or contain the damage from the attack.	The asset is likely to resist, withstand, or contain the damage from the attack	The asset is somewhat likely to resist, withstand, or contain the damage from the attack.	The asset is unlikely to resist, withstand, or contain the damage from the attack.	The asset is very unlikely to resist, withstand, or contain the damage from the attack.

The variable used for the likelihood of vulnerability to an attack method,  $V_p$ , is based on government expert judgments of three factors.

- **Recognizability (Rg):** The likelihood that the adversary will be able to identify and locate the asset and its significance, taking into consideration labeling, signage, press, uniqueness, and the adversary’s knowledge.
- **Countermeasure Effectiveness (Ce):** The effectiveness of the countermeasures protecting the asset, specifically in the areas of denial, detection, and interdiction.
- **Robustness / Resistance (Rs)** The asset’s or system’s level of ability to sustain the attack without countermeasures, due to inherent resistance, system resistance, and independence.

Each component is ranked on a 0 to 4 scale, and each ranking is assigned a value in the range of 0 to 1. As with threat, the intervals between the values assigned to each level of vulnerability are set to represent analytic judgments of their contributions to an overall vulnerability level. These values are multiplied, hence,

$$V_p = R_g \times C_e \times R_s \text{ (Equation 6)}$$

The final number provides an indication of the relative severity of the vulnerability for each attack scenario and represents a probability that an attack will succeed.

*Consequence*

To assess consequences, SSAs consider loss of life, economic losses, and the psychological or behavioral impact of an attack, as described in each attack method, in a worst, reasonable case scenario. Ranking tables are then used to standardize responses and assign values that range from negligible consequence to catastrophic national consequences.

<b>Component</b>	<b>Ranking Level (SHIRA Severity)</b>				
	<b>0 None/ Negligible</b>	<b>1 Minor</b>	<b>2 Moderate</b>	<b>3 Significant</b>	<b>4 Catastrophic/ Severe</b>
<b>Loss of Life</b>	Attack likely to produce no fatalities	Attack likely to cause less than 100 fatalities	Attack likely to cause greater than 100 fatalities	Attack likely to cause greater than 1,000 fatalities	Attack likely to cause greater than 10,000 fatalities
<b>Economic Losses</b>	Estimated costs from the attack are likely less than \$100 million	Estimated costs from the attack are relatively minor, in the range of \$100 million to \$1 billion	Estimated costs from the attack in the range of \$1 billion to \$10 billion	Estimated costs from the attack in the range of \$10 billion to \$100 billion	Estimated costs from the attack in excess of \$100 billion
<b>Psychological / Behavioral Impact</b>	No major change in population behavior, or effects on social functioning locally or nationally.	Occasional or minor loss of nonessential social functions in a circumscribed geographical area.	Loss of many nonessential social functions in a circumscribed geographical area.	Dysfunctional behavior and disruption of important social functions for a sustained period.	Loss of belief in government and institutions; widespread disregard for official instructions; widespread looting and civil unrest.

The consequence of a potential terrorist act is based on several constituent components: loss of life, economic losses, and the psychological impact on the populace, and is represented by the variables **L**, **E**, and **Ps**, respectively. The estimates can be based on expert opinion, quantitative assessments, if available, or modeling and simulation, if applicable. The framework ranks these components from 0 through 4. These component values are added for a cumulative total and normalized. The final number provides an indication of the relative consequence for each attack scenario.

The consequence rankings are measures of severity in the context of the SHIRA and are assessed on a common interval scale, where the assessed severity is equivalent within each column and rises linearly from one description to the next in each row. The broad range in each severity level is a result of the scope of the SHIRA, a national level assessment inclusive of all CIKR sectors. The interval scale also allows for a national level risk framework that can incorporate more granular assessments of specific assets and systems. The components of consequence follow a logical progression for national level consequences horizontally; vertically, the severity levels provide levels of equivalency that reflect the current decision-making judgment of the DHS. These equivalencies can be modified based upon decision-maker input.

To get the total consequence, the SHIRA takes the average of the consequence components:<sup>17</sup>

$$C = (L + E + P) / 3 \text{ (Equation 7)}$$

The SHIRA model normalizes the consequence to a range of 0-100 by multiplying by 25:

$$C = [(L + E + P) / 3] * 25 \text{ (Equation 8)}$$

### *Combining the Components for Risk*

To produce the final value for the risk of the scenario, the SHIRA multiplies the value for consequence from Equation 8 by the probability that the scenario will occur, which in the SHIRA is the product of the threat and vulnerability variables.

In this view, the process of computing the value of risk is equivalent to calculating the expected value of a random variable with two possible states – C, the consequence of the attack scenario succeeding, and 0, the consequence of the attack scenario not succeeding.<sup>18</sup> Thus:

$$R = \text{Prob(attack does not succeed)} * 0 + \text{Prob(attack succeeds)} * C \text{ (Equation 9)}$$

$$R = \text{Prob(attack succeeds)} * C \text{ (Equation 10)}$$

$$R = (T * V) * C \text{ (Equation 11)}$$

In this context, the risk value is the expected severity of the consequence.

### **Path Forward**

The SHIRA is a semi-quantitative risk assessment that utilizes tables as guidance for the IC and infrastructure protection community representatives to estimate the components of threat, vulnerability, and consequence. The success of the SHIRA comes from understanding of the requirements for a national CIKR risk assessment coupled with the constraints and limitations of processes, products, people, and technology. The threat rankings provided by the interagency coordination of the IC are the basis for a DHS assessed probability for each ranking. Likewise, the vulnerability rankings provided by the Sector Specific Agencies that represent each CIKR sector, are converted to probabilities by DHS. Additional enhancements to the threat and vulnerability components should focus on the core principles of sound risk analysis. For example, as

---

<sup>17</sup> Because we consider severity to increase linearly from one linguistic description of each component to the next, averaging is a proper way to obtain a unified measure for consequence severity.

<sup>18</sup> Such a variable is called a Bernoulli random variable and its expected value is  $E[\text{variable}] = \text{Prob}(\text{State1}) * \text{Value}(\text{State1}) + \text{Prob}(\text{State2}) * \text{Value}(\text{State2})$ .

the data become more readily available to DHS, more detailed tables that standardize probabilities associated with the tables will produce more repeatable results. The consequence estimates are based upon large nationally significant ranges; similarly, future enhancements should focus on refining the ranges to allow an easier integration of more detailed analysis.

Several terrorist attack scenarios exist that could lead to consequences not captured under Loss of Life, Economic Losses, or Psychological Impacts factors. For example, while a single attack on a Defense Industrial Base asset could cause health, economic, and psychological impacts, the primary consequences may be a hindrance to the military's operational capacity. Consequently, mission disruption should be added as a fourth consequence factor that could enable all SSAs to account for the impact of an attack on national security and federal operations, public health and safety, and essential public services.<sup>19</sup> By evaluating these effects, the SHIRA could compile a more complete picture of the risk to the nation's CIKR.

The current scope of the SHIRA focuses the assessment of terrorism risk at the strategic level. Although it will remain there, the enhancements and refinements to the model should allow for integration with other models more pertinent for operational and tactical levels. As risk assessments to specific assets and systems proliferate within the infrastructure protection community, DHS should identify and exploit areas of integration. Horizontal and vertical integration of risk analysis and data will provide the backbone for a shared understanding and communication of risk at all levels. Horizontal integration requires information sharing (data, analysis, knowledge) not only within the infrastructure protection or intelligence domains, but also throughout all the components of DHS. The Science and Technology Directorate, for example, provides DHS access to the research capabilities of the nation's universities through the Centers of Excellence. Integration with new research and technology will enable the current practices to reduce the constraints and limitations of current models.

---

<sup>19</sup> Although the definitions in the guidance documents seem to focus exclusively on governmental functions, the mission areas described go beyond the public sector. Services such as the "orderly functioning of the economy" involve private organizations in the banking and finance sector; the provision of drinking water is an essential service, and in many cases utilities are private entities.

The definitions used in Homeland Security Presidential Directive-7, the National Infrastructure Protection Plan, and the Homeland Security Act have areas of overlap. To help create a mission disruption–consequence factor, the SHIRA team simplified the six components into three groups of mission impacts:

- **Federal and National Security Impact** includes the first two missions (Ensure National Security, Perform Federal Missions) because they both focus on a national scale.
- **Public Health and Safety Impact** includes the next two components (Ensure Public Health and Safety, Maintain Order) because maintaining order is an integral part of ensuring public health and safety.
- **Provide Essential Public Services** group the remaining two components (Provide Essential Public Services, Ensure Orderly Economy) because the best way to ensure an orderly functioning economy is to provide essential public services, especially safe, secure, and reliable banking and finance services.

## **Conclusion**

The foundation of threat-based risk analysis in the SHIRA can serve as the bedrock of future terrorism risk analysis to critical infrastructure at DHS. As the accessibility to critical infrastructure data increases and as the IC becomes more familiar with the infrastructure protection community's needs, the quality of the risk analysis will improve with the more granular or more direct data. The "fusion" concept, under which the SHIRA is produced, if nurtured and allowed to develop into its full potential, will help DHS to fully realize a nascent culture. The SHIRA is a model, methodology, and product developed through the interactions of the various communities of interest along the common thread of threat-based analysis. Its success serves as a microcosm of homeland security: a success based upon the interactions of once disparate entities brought together under a single focus.

Information sharing and collaboration are the fulcrums on which terrorism risk analysis depend; the communities of interest in both the IC and the infrastructure protection community provide a depth and breadth of knowledge that only DHS can harness. DHS alone is the organization that can bring together the private and public sectors of the infrastructure protection community; DHS alone is the organization that can, through its own intelligence organization, bring the IC to the infrastructure protection community; and DHS alone is the organization that can synthesize the data and analysis together to formulate a terrorism risk assessment for critical infrastructure protection. As DHS grows beyond five years, we can assume that information sharing and collaboration will increase and improve between all stakeholders. This will lead to more data to analyze; more data, however, do not indicate better data and better data do not point to better analysis. Greater accessibility to data – both intelligence and critical infrastructure – will allow for more rigorous analysis of terrorism risk and finer granularity in the assessments. The threat-based terrorism risk analysis being cultivated today through projects like the SHIRA will allow DHS to harvest plentifully in the future.



**AUTHOR BIOGRAPHY**

Geoffrey French is a Program Manager for CENTRA Technology, Inc, and currently supports strategic risk analysis for the U.S. Department of Homeland Security. Mr. French has supported counterintelligence analysis and operations for the Federal Bureau of Investigation and the U.S. Department of Defense. He has a B.A. in History from Wichita State University and an M.A. in National Security Studies from Georgetown University. He is a founding member of the Security Analysis and Risk Management Association.

**AUTHOR BIOGRAPHY**

Jin Kim is an Analyst for CENTRA Technology, Inc, and currently supports strategic risk methodology and analysis for the U.S. Department of Homeland Security. Mr. Kim has worked in the intelligence community for over ten years -- from tactical Army assignments to strategic assignments supporting the Department of Defense. He has a B.S. in General Engineering from the United States Military Academy and an M.A. in Security Studies from the School of Foreign Service at Georgetown University.

**AUTHOR BIOGRAPHY**

Pasha Vasilev is an Analyst for CENTRA Technology, Inc, and currently supports a variety of analytical and open source research projects. Mr. Vasilev has worked on assignments involving mathematics and technology for more than five years. He has a B.A. in Computer Science from Harvard University and an M.A. in Law and Diplomacy from The Fletcher School at Tufts University.



**The Mathematics of Terrorism Risk:**  
**Equilibrium Force Allocations and Attack Probabilities**

**Bruce I. Gudmundsson**

Senior Fellow for Case Studies  
Marine Corps University

**Michael R. Powers**

Professor of Risk Management and Insurance, Fox School of Business  
Temple University

Distinguished Visiting Professor of Finance, School of Economics and Management  
Tsinghua University

[May 15, 2008]

**Abstract**

We model the struggle between terrorist and conventional forces as a *Colonel Blotto* game, replacing Powers and Shen's (2006) mathematical expression for the probability of target destruction by a more rigorously derived approximation from a diffusion-based Lanchester analysis. We then use the resulting equilibrium solutions for force allocations and attack probabilities to make inferences about terrorist attackers and government defenders that are roughly consistent with empirical findings. Our analysis reveals that the loss function of a government/society plays a central role in determining the types of targets likely to be attacked by terrorists in "peacetime" and "wartime", leading to a much more frequent selection of "trophy" targets in peacetime.

**Keywords** – Terrorism risk, force allocations, attack probabilities, game theory, Lanchester equations, power-law distributions.

## 1. Introduction

To study the problem of terrorism risk, we model the struggle between terrorist and conventional forces as a *Colonel Blotto* game. This approach arises from the confluence of three distinct research streams: (1) the game-theoretic analyses of terrorism provided by Major (2002) and Powers and Shen (2006); (2) the introduction of diffusion processes into Lanchester-like combat analyses, first proposed by Perla and Lehoczky (1977), and more recently developed by Powers (2008) and Gudmundsson et al. (2008); and (3) the empirical analysis of terrorist-destroyed-target distributions conducted by Johnson et al. (2005). Given that many of the relevant mathematical theorems are published elsewhere, we confine the present study primarily to the implications of those results, and provide all new derivations in a technical appendix.

Most significantly, we replace Powers and Shen's (2006) mathematical expression for the conditional probability of destruction of a target, given that that target is selected for attack by terrorists, by a more rigorously derived approximation from a diffusion-based Lanchester analysis. We then use the resulting equilibrium solutions for force allocations and attack probabilities to make inferences about terrorist attackers and government defenders that are roughly consistent with the empirical findings of Johnson et al. (2005). In addition to providing explicit forms for the force-allocation and attack-probability strategies, our analysis reveals that the loss function of a government (*qua* society) plays a central role in determining the actions of attackers. Distinguishing between the risk attitudes of "peacetime" and "wartime" governments, we find that there is a much more frequent selection of "trophy" targets in peacetime.

## 2. Prior Work

### 2.1. The *Colonel Blotto* Game

Given a finite set of potential targets, let  $W$  denote the combined monetary/human-life value<sup>[1]</sup> of a particular target, which is assumed to be directly proportional to that target's (three-dimensional) physical volume,  $V$ ; that is,  $W \propto V$ . Next, let  $A$  and  $D$  denote the sizes of the forces allocated to the target by the terrorist attackers and government defenders, respectively, where the attackers' (but not the defenders') *total* forces are assumed to be fixed *a priori*.

In the *Colonel Blotto* game, the attackers and the defenders must allocate their total forces across the various targets without knowing their opponents' strategies. In the simplest version of the game, the player that assigns the higher level of force to a given target prevails at that target; in a more sophisticated version, a player's probability of prevailing would be an increasing function of the player's force allocation (for a fixed allocation made by the player's opponent). For our purposes, we will say that the attackers prevail at a given target if they succeed in destroying the target, and that the defenders prevail by preserving the target, while explicitly acknowledging that any target that is attacked is *partially* damaged. A player's payoff from the game is then the expected value of that player's total gain or loss from the outcomes at the various targets.

Powers and Shen (2006) proposed that the attackers' conditional probability of destroying a particular target, given that that target is selected for attack, be written as

$$p = \exp\left(-\frac{A^s D^s}{V^s}\right) \left(\frac{A^c}{A^c + D^c}\right), \quad (1)$$

---

[1] The use of a hybrid monetary *and* human-life value scale is a quantitative simplification that bears further study. For the present, one could think of  $W$  as consisting of two components, one for monetary worth and one for human lives, and simply assume that the two components always increase or decrease in direct proportion to each other.

where the first factor on the right-hand side of equation (1) represents the probability that the attackers avoid detection prior to their attack (derived from a simple search model), and the second factor represents the probability that the attackers are then successful in destroying the target (derived from a classical gambler's ruin model). In the above expression, the constants  $s > 1$  and  $0 < c < 1$  are scale parameters. Powers and Shen (2006) also assumed that the attackers' gain associated with damage to, and/or destruction of, a target of physical volume  $V$  is given by  $Gain_A(V) \propto V^\lambda$ , for some positive constant  $\lambda$ , and that the game is zero-sum (so that the defenders' corresponding loss is given by  $Loss_D(V) \propto V^\lambda$ ). They then used equation (1) to prove three theorems.

The first theorem addresses the case in which terrorists attack all of the targets simultaneously, and shows that there exists a Cournot-Nash equilibrium in which both the attackers and defenders allocate their forces to each target in direct proportion to the square root of the target's volume. The second theorem addresses the case in which terrorists attack only one target, selected at random, and shows that there exists a Cournot-Nash equilibrium in which both sides again allocate their forces in direct proportion to the square roots of a target's volume. Finally, the third theorem reveals that if the probability with which the attackers select a target at random (in the setting of the second theorem) is treated as a strategic decision of the attackers, then no Cournot-Nash equilibrium with pure-strategy force allocations can exist.

Given that the setting of the second theorem appears more relevant to today's War on Terror, we will work with that model in the present study. However, because of potential weaknesses with the expression in equation (1) (e.g., the right-hand side approaches zero as  $A$

tends to infinity)<sup>[2]</sup>, we will replace that probability with a more rigorously derived expression based upon a stochastic Lanchester model tailored specifically to terrorism combat.

## 2.2. The Lanchester Paradigm

The most widely studied mathematical model of military combat is that proposed by Lanchester (1916), which may be described by a system of differential equations of the form

$$dA = -k_1 A^{\alpha_1} D^{\delta_1} dt \quad (2)$$

$$dD = -k_2 A^{\alpha_2} D^{\delta_2} dt, \quad (3)$$

where:  $A = A(t)$  and  $D = D(t)$  denote, respectively, the sizes of the attackers' and defenders' forces at time  $t \geq 0$ ;  $k_1, k_2$  are positive constants denoting, respectively, the defenders' and attackers' effective destruction rates; and  $\alpha_1, \alpha_2$  and  $\delta_1, \delta_2$  are real-valued constants reflecting the fundamental nature of the combat under study. In his original formulation, Lanchester (1916) considered two cases – one for “ancient” warfare, in which  $\alpha_1 = 1, \delta_1 = 1, \alpha_2 = 1, \delta_2 = 1$ , and one for “modern” warfare, in which  $\alpha_1 = 0, \delta_1 = 1, \alpha_2 = 1, \delta_2 = 0$ .

Gudmundsson et al. (2008) considered a special case of (2) and (3) designed specifically for terrorism combat:

$$dA = -\frac{k'_1}{V^q} ADdt \quad (4)$$

$$dD = -k_2 Adt, \quad (5)$$

where:  $V$  (as before) denotes the physical volume of the target under attack;  $q$  denotes a positive power-transformation constant used to recognize the appropriate domain of combat (e.g.,  $q = 1/3$  if a building can be attacked through only its ground-level perimeter,  $q = 2/3$  if a

---

<sup>[2]</sup> This means that as the terrorists' forces increase in magnitude, the disadvantage of size in terms of avoiding detection eventually outweighs the benefit of size in combat. While this implication may be realistic in certain scenarios, it is easily challenged. For example, the September 11 attacks suggest a small role for detection in even the boldest of attacks when the target is inadequately defended.

building can be attacked anywhere along its surface, as by a fuel-filled airplane, and  $q = 1$  if a bomb can be planted anywhere within a building); and  $k'_1 = k_1 V^q$ . Rewriting  $A$  and  $D$  in terms of a single variable,  $U(A, D)$ , Gudmundsson et al. (2008) replaced the system (4), (5) with the stochastic differential equation

$$dU = Udt + \sigma U^{\gamma/2} dZ,$$

where:  $dZ$  is a standard Brownian motion;  $\sigma$  is the associated infinitesimal standard deviation; and  $\gamma \in [0, 2]$ . They then identified the attackers' probability of victory with the probability of first-passage to the state  $D = 0 \Leftrightarrow U = 1$ , and derived the following approximation for the attackers' conditional probability of destroying a particular target, given that that target is selected for attack:

$$p = \begin{cases} 1 - \frac{k'_1 D^2}{2k_2 V^q A} & \text{for } A > \frac{k'_1 D^2}{2k_2 V^q} \\ 0 & \text{for } A \leq \frac{k'_1 D^2}{2k_2 V^q} \end{cases}. \quad (6)$$

### 3. Analytical Results

Substituting equation (6) for equation (1) in a modified version<sup>[3]</sup> of Powers and Shen's (2006) second theorem, we obtain the following result. (The proof is provided in the appendix.)

**Theorem 1:** There exists a Cournot-Nash equilibrium in which the attackers' and defenders' force allocations to a particular target are given by  $A \propto W^a$  and  $D \propto W^d$ , respectively, and the attackers' probability of selecting the target is given by  $\pi \propto W^r$ , for constants  $a$ ,  $d$ , and  $r$  such that the probability of target destruction ( $p$ ) is 0.

---

<sup>[3]</sup> In addition to the stated revision of the target-destruction probability, our analysis differs from Powers and Shen's (2006) in that (1) the defenders' total forces are not fixed *a priori*, and (2) every target that is attacked is assumed to be partially damaged.



Although Theorem 1 states that no target can be destroyed in equilibrium, it is important to recall our assumption that any target attacked will be partially damaged. Obviously, the occurrence of another September 11-like event, in which major targets are destroyed completely, would cast serious doubt on the validity of the above result.<sup>[4]</sup> However, any attack with only partial damage would be consistent with it.

From the first-order conditions of the optimization problem underlying Theorem 1 (shown in the proof), we know that the result is subject to the constraints

$$2d + r + \lambda = q + 2a \tag{7}$$

and

$$d = (q + a)/2. \tag{8}$$

Assuming that  $q$  and  $\lambda$  are known, this leaves three unknown constants –  $d$ ,  $a$ , and  $r$  – but only two equations – (7) and (8) – to specify them.

Fortunately, there is one additional piece of information that we have not yet used – the fact that in a real-world *multi-period* setting, the attackers are able to move first (e.g., with the September 11 strikes), and thus are able to select the equilibrium constant  $r$  (which the defenders then are forced to follow in all subsequent plays of the game). Given the privilege of selecting this constant, the attackers will do so in a way that maximizes the *expected value* (or average value) of their gain – that is, the weighted sum of  $Gain_A$  over all of the targets, where each target is weighted by its corresponding probability of partial damage (i.e., its probability of being attacked, since there is no chance of target destruction under Theorem 1).

---

<sup>[4]</sup> In fact, for Theorem 1 to be consistent with reality, one must view the September 11 attacks as a formal initiation of hostilities, only after which the *Colonel Blotto* game actually began.

Assuming, as suggested by the empirical work of Kaizoji and Kaizoji (2008), that the distribution of available target values follows a continuous power law with positive constant  $t$ ,<sup>[5]</sup> it is not difficult to derive the following result (proved in the appendix).

**Theorem 2:** For the Cournot-Nash equilibrium described in Theorem 1, the attackers can maximize their expected gain by choosing

$$r = t' - 1 - \lambda, \quad (9)$$

for any constant  $t'$  that is greater than or equal to  $t$ .

Substituting equation (9) into equations (7) and (8) then yields

$$a = t' - 1 \quad (10)$$

and

$$d = (q + t' - 1)/2. \quad (11)$$

#### 4. Discussion

In light of equations (9) through (11), our Cournot-Nash-equilibrium result may be restated as follows.

**Corollary 1:** There exists a Cournot-Nash equilibrium in which the attackers' and defenders' pure-strategy force allocations to a particular target are given by  $A \propto W^{t'-1}$  and  $D \propto W^{(q+t'-1)/2}$ , respectively, and the attackers' probability of selecting the target is given by  $\pi \propto W^{t'-1-\lambda}$ .

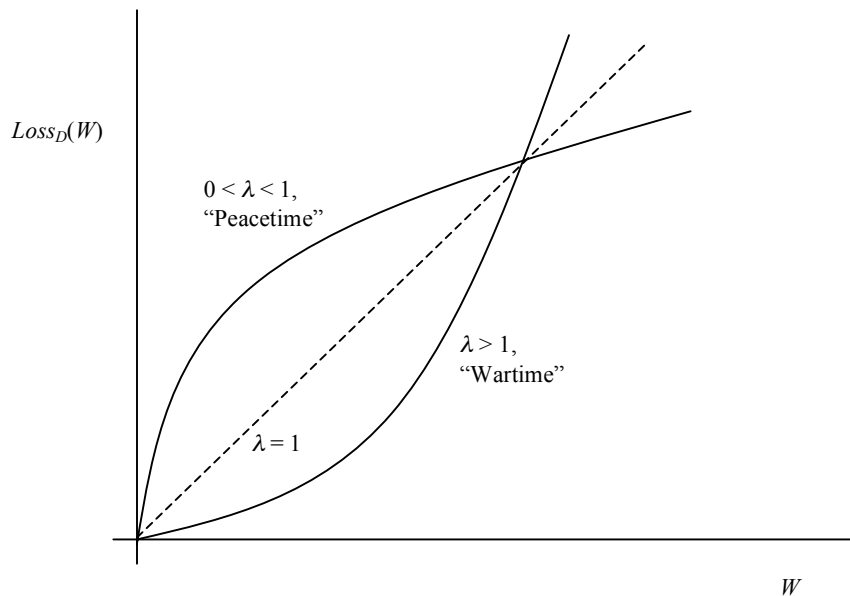
To interpret this result, we must know something about the positive constants  $q$ ,  $t'$ , and  $\lambda$ . For simplicity, we will assume that  $q = 1$  – that is, that the domain of combat includes the entire three-dimensional volumes of the targets. Furthermore, consistent with Kaizoji and

---

<sup>[5]</sup> Formally, this means that the probability density function of available target values is given by  $f(W) \sim W^{-t}$ .

Kaizoji (2008), we will assume that  $t = 2.35$  for industrially developed nations,<sup>[6]</sup> and further that  $t' = t = 2.35$ . (In less-developed nations, one would expect the value of  $t'$  to be somewhat larger, since the distribution of property values would tend to have a thinner tail.) This leaves the gain/loss-function constant,  $\lambda$ , for further investigation.

Consider then the government defenders' loss function,  $Loss_D(W) \propto W^\lambda$ . Figure 1 shows that this function is: (1) concave downward for values of  $\lambda$  between 0 and 1; (2) linear for  $\lambda = 1$ ; and (3) concave upward for values of  $\lambda$  greater than 1. At first blush, it seems reasonable that the loss function should be concave downward, since a government would tend to experience decreasing marginal losses as the monetary/human-life values of the terrorists' targets increase. For example, one might argue that for the U.S. government's September 11 losses to be doubled, the terrorists would have to destroy a target of more than twice the monetary/human-life value of the September 11 targets.



**Figure 1. Government's Loss Function for Various Values of  $\lambda$**

<sup>[6]</sup> Kaizoji and Kaizoji (2008) provided annual estimates of  $t$  for Japanese land values during the period 1981-2002. Those estimates vary from a low of about 2.0 to a high of about 2.7. We have selected the approximate sample mean (2.35) of the estimates for our analysis.

Note, however, that a concave-downward function corresponds to an assumption of *risk proneness* on the part of the government defenders (i.e., given the choice between any random lottery and a fixed amount equal to the lottery's expected value, they would prefer the lottery itself). Thus, such an assumption appears somewhat inconsistent with the generally observed *risk-averse* nature of governments (e.g., their seemingly cautious behavior in responding to life-threatening crises).

To place this issue in some perspective, one might distinguish between two distinctly different societies, one – like the U.S. – that has enjoyed a long period of domestic peacetime, and another – like Israel – that has experienced an extensive period of terrorist activity. While it is true that *all* governments, in moments of crisis, manifest risk-averse tendencies, such behavior is not necessarily characteristic of more mundane periods. More precisely, in a nation used to peace, it is quite likely that – apart from specific moments of crisis – both the populace and government tend to “take chances” by preferring an abundance of personal liberty and relaxed government security. In a nation used to war, however, a more restrictive, security-conscious view would tend to prevail even in the best of times.

For these reasons, it makes sense to model the U.S. and other “peacetime” governments as risk-prone decision makers (with concave-downward loss functions; i.e.,  $0 < \lambda < 1$ ), while modeling the Israeli and other “wartime” governments as risk-averse decision makers (with concave-upward loss functions; i.e.,  $\lambda > 1$ ). Hypothetically, we will select  $\lambda = 0.5$  for peacetime nations and  $\lambda = 1.5$  for wartime nations.<sup>[7]</sup>

---

<sup>[7]</sup> Note that, under our zero-sum assumption, the selection of the defenders' loss function immediately implies the form of the attackers' gain function. This is quite reasonable if the attackers' utility (gratification) arises directly from the defenders' disutility (frustration).

We now return to the above Cournot-Nash-equilibrium result and suggest that, in practice, one should expect to find results similar to the following (in industrially developed nations):

$$A \propto W^{t'-1} = W^{1.35}, \quad (12)$$

$$D \propto W^{(q+t'-1)/2} = W^{1.175}, \quad (13)$$

$$\pi \propto W^{t'-1-\lambda} = \begin{cases} W^{0.85} & \text{for peacetime nations} \\ W^{-0.15} & \text{for wartime nations} \end{cases} \quad (14)$$

To compare these implications with the empirical distributions of *destroyed* (rather than simply *available*) target values estimated by Johnson et al. (2005),<sup>[8]</sup> one first must multiply  $\pi$  (for wartime nations) by the probability density function associated with a power-law constant of  $t$ . This yields

$$g(W) \propto \pi f(W) \sim W^{t'-1-\lambda-t} = W^{-2.5}. \quad (15)$$

Interestingly, the constant in the power-law distribution implied by approximation (15),  $\tau = 2.5$ , happens to be identical to the constant estimated by Johnson et al. (2005) for less-developed wartime nations. However, our figure is substantially higher than Johnson et al.'s (2005) estimate for industrially developed wartime nations ( $\tau = 1.71$ ) (although the latter estimate could be obtained quite readily by changing the assumption of  $t' = 2.35$  to the equally permissible  $t' = 3.14$ ).

Given the highly subjective procedure for selecting the various model constants ( $q$ ,  $t'$ , and  $\lambda$ ), one should not read too much into either of these comparisons. Rather, we simply would observe that our results appear to be in the same ballpark as Johnson et al.'s (2005), which

---

<sup>[8]</sup> Johnson et al. (2005) argued that the distribution of destroyed target values follows a continuous power law with positive constant  $\tau$  (i.e., the probability density function is given by  $g(W) \sim W^{-\tau}$ ). They further estimated the values of  $\tau$  for both industrially developed nations and less-developed nations.

affords some support for the following *qualitative* observations from approximations (12) through (14):

- In both peacetime and wartime, government defenders tend to allocate forces in slightly lower proportion to high-value targets than do terrorist attackers.
- In peacetime, terrorist attackers tend to give substantial weight to high-value targets; however, such targets actually are avoided in wartime.

## 5. Conclusions

In the present study, we have modeled the struggle between terrorist and conventional forces as a *Colonel Blotto* game. We first replaced Powers and Shen's (2006) mathematical expression for the conditional probability of destruction of a particular target, given that that target is selected for attack by terrorists, by a more rigorously derived approximation from a diffusion-based Lanchester analysis, and then used the resulting equilibrium solutions for force allocations and attack probabilities to make inferences about terrorist attackers and government defenders. A brief analysis showed that these solutions are roughly consistent with the empirical findings of Johnson et al. (2005).

Our analysis revealed that the loss function of a government plays a central role in determining the types of targets likely to be attacked by terrorists in "peacetime" and "wartime", respectively. Specifically, we found that terrorists tend to select high-value ("trophy") targets much more frequently in peacetime than in wartime.

Investigating how a government's loss function depends on its society's perception of conflict-related risk is crucial to a thorough understanding of the behavior of both governments and terrorists. We believe this is a promising area for further research.

## References

- Gudmundsson, B. I., Powers, M. R., and Zhang, L. (2008), “The mathematics of terrorism risk: Lanchester SDEs and the probability of target destruction,” working paper, Center for Insurance and Risk Management, Tsinghua University.
- Johnson, N. F., Spagat, M., Restrepo, J. A., Becerra, O., Bohórquez, J. C., Suárez, N., Restrepo, E. M., and Zarama, R. (2005), “Universal patterns underlying ongoing wars and terrorism,” *arXiv:physics/0506213v1*, available at <http://xxx.lanl.gov/abs/physics/0506213>.
- Kaizoji, T. and Kaizoji, M. (2008), “A mechanism leading from bubbles to crashes: the case of Japan’s land market,” *arXiv:cond-mat/0312404v2*, available at <http://arxiv.org/abs/cond-mat/0312404v2>.
- Lanchester, F. W. (1916), “Aircraft in warfare: the dawn of the fourth arm – the principle of concentration,” *Engineering*, Vol. 98, pp. 422-423.
- Major, J. A. (2002), “Advanced techniques for modeling terrorism risk,” *Journal of Risk Finance*, Vol. 4, No. 1, pp. 15-24.
- Perla, P. P. and Lehoczky, J. P. (1977), “A new approach to the analysis of stochastic Lanchester processes – time evolution,” technical report, Carnegie-Mellon University Department of Statistics.
- Powers, M. R. (2008), “Lanchester resurgent? the mathematics of terrorism risk,” *Journal of Risk Finance*, Vol. 9, No. 3.
- Powers, M. R. and Shen, Z. (2006), “Colonel Blotto in the war on terror: implications for event frequency,” paper presented at the American Risk and Insurance Association Annual Meeting, Washington, DC.

## Appendix

### Proof of Theorem 1:

Let  $i = 1, 2, \dots, n$  be the index for the various targets, and let

$$E[Gain_A] = \sum_{i=1}^n \pi_i(\varepsilon_A + p_i k_A) V_i^\lambda = \sum_{i=1}^n \pi_i(\varepsilon_A + p_i k_A) v^\lambda W_i^\lambda \text{ and}$$

$$E[Loss_D] = \sum_{i=1}^n \pi_i(\varepsilon_D + p_i k_D) V_i^\lambda = \sum_{i=1}^n \pi_i(\varepsilon_D + p_i k_D) v^\lambda W_i^\lambda,$$

where:  $\varepsilon_A, \varepsilon_D$  are positive constants reflecting the amount of partial damage sustained by any target that is attacked;  $k_A, k_D$  are positive constants reflecting the additional damage sustained by a target that is destroyed;  $v$  is a positive constant such that  $vW_i = V_i$ ; and

$$p_i = 1 - \frac{k_1' D_i^2}{2k_2 V_i^q A_i} = 1 - \frac{k_1' D_i^2}{2k_2 v^q W_i^q A_i}. \text{ To solve the joint optimization problem}$$

$$\text{Max}_{A_1, \dots, A_n} E[Gain_A] \quad \text{s.t.} \quad \sum_{i=1}^n A_i = A^* \text{ and}$$

$$\text{Min}_{D_1, \dots, D_n} E[Loss_D] \quad \text{s.t.} \quad \sum_{i=1}^n D_i < \infty,$$

where  $A^*$  is a positive constant denoting the attackers' total forces (fixed *a priori*), we seek solutions satisfying

$$\text{grad}(E[Gain_A]) - \mu_A \text{grad}\left(\sum_{i=1}^n A_i\right) = 0 \text{ and}$$

$$\frac{\partial E[Loss_D]}{\partial D_i} = 0 \text{ for } i = 1, 2, \dots, n,$$

where  $\mu_A$  is a Lagrange multiplier. In other words, we wish to solve the system of first-order equations



$$\frac{\partial p_i}{\partial A_i} \pi_i k_A v^\lambda W_i^\lambda = \mu_A \text{ and} \quad (\text{A1})$$

$$\frac{\partial p_i}{\partial D_i} \pi_i k_D v^\lambda W_i^\lambda = 0 \quad (\text{A2})$$

for  $i = 1, 2, \dots, n$ , subject to the second-order conditions

$$\frac{\partial^2 E[\text{Gain}_A]}{\partial A_i^2} = \frac{\partial^2 p_i}{\partial A_i^2} \pi_i k_A v^\lambda W_i^\lambda < 0 \text{ and} \quad (\text{A3})$$

$$\frac{\partial^2 E[\text{Loss}_D]}{\partial D_i^2} = \frac{\partial^2 p_i}{\partial D_i^2} \pi_i k_D v^\lambda W_i^\lambda > 0 \quad (\text{A4})$$

for  $i = 1, 2, \dots, n$ .

Now let  $A_i = \alpha W_i^a$  and  $D_i = \delta W_i^d$  denote the equilibrium-allocation solutions, where

$$\alpha = A^* / \sum_{j=1}^n W_j^a,$$

and let  $\pi_i = \rho W_i^r$  denote the attackers' probability of selecting target  $i$ , where

$$\rho = 1 / \sum_{j=1}^n W_j^r.$$

Since

$$\frac{\partial p_i}{\partial A_i} = \frac{k_1' D_i^2}{2k_2 v^q W_i^q A_i^2},$$

it follows from equation (A1) that

$$\frac{k_1' D_i^2}{2k_2 v^q W_i^q A_i^2} \rho W_i^r k_A v^\lambda W_i^\lambda = \frac{k_1' \delta^2 W_i^{2d}}{2k_2 v^q W_i^q \alpha^2 W_i^{2a}} \rho W_i^r k_A v^\lambda W_i^\lambda = \mu_A. \quad (\text{A5})$$

Then, since inequality (A3) always holds, we can collect the exponents of  $W_i$  in equation (A5) to conclude

$$2d + r + \lambda = q + 2a.$$

Turning to the defenders' allocations, we note that

$$\frac{\partial p_i}{\partial D_i} = -\frac{k'_1 D_i}{k_2 v^q W_i^q A_i}$$

is negative for all  $D_i > 0$ , and so there is no internal solution to equation (A2) (and indeed, inequality (A4) also fails). Consequently, the values of  $D_i$  that minimize  $E[Loss_D]$  must lie at the boundary provided by equation (6); that is,

$$D_i = \sqrt{\frac{2k_2 v^q W_i^q A_i}{k'_1}} = \sqrt{\frac{2k_2 v^q \alpha}{k'_1}} W_i^{(q+a)/2},$$

for which  $p_i = 0$ . This implies

$$\delta = \sqrt{\frac{2k_2 v^q \alpha}{k'_1}} \text{ and}$$

$$d = (q + a)/2.$$

### Proof of Theorem 2:

From the proof of Theorem 1, we know that

$$E[Gain_A] = \sum_{i=1}^n \pi_i (\varepsilon_A + p_i k_A) v^\lambda W_i^\lambda = \sum_{i=1}^n \rho W_i^r \varepsilon_A v^\lambda W_i^\lambda = \left( \varepsilon_A v^\lambda / \sum_{j=1}^n W_j^r \right) \sum_{i=1}^n W_i^{r+\lambda}.$$

Given that the distribution of  $W_i$  is continuous with probability density function

$$f(W) \sim W^{-t},$$

it follows that

$$f(W) \propto (W + c)^{-t}$$

for some positive constant  $c$ , and

$$E[Gain_A] = \left( \varepsilon_A v^\lambda / nE[W_i^r] \right) nE[W_i^{r+\lambda}] = \varepsilon_A v^\lambda \left( E[W_i^{r+\lambda}] / E[W_i^r] \right)$$

$$= \varepsilon_A v^\lambda \frac{\int_0^\infty W^{r+\lambda}(W+c)^{-t} dW}{\int_0^\infty W^r(W+c)^{-t} dW},$$

which is finite for  $r < t - 1 - \lambda$  and diverges to positive infinity for  $r \geq t - 1 - \lambda$ . (Actually, the above ratio of integrals possesses the indeterminate form  $\infty/\infty$  for  $r \geq t - 1$ , but one can interpret

this as divergence to positive infinity by viewing  $\frac{\int_0^\infty W^{r+\lambda}(W+c)^{-t} dW}{\int_0^\infty W^r(W+c)^{-t} dW}$  as

$\lim_{z \rightarrow \infty} \frac{\int_0^z W^{r+\lambda}(W+c)^{-t} dW}{\int_0^z W^r(W+c)^{-t} dW}$  and applying l'Hôpital's rule.)



**A Service Oriented Approach (SOA) to the  
IT-based Protection of Critical Infrastructures-  
A First Approach to Integrate SOA into a Complex Operational Analysis  
within Risk Assessment and Risk Management Processes**

Razvan Bugheanu, Marius Dumitrascu  
Goran Mihelcic, Stefan Pickl

Department of Computer Science  
Chair for Operations Research  
University of the Federal Armed Forces Munich

<http://www.unibw.de/stefan.pickl>  
[Stefan.Pickl@unibw.de](mailto:Stefan.Pickl@unibw.de)

Germany-85577 Neubiberg-München

**ABSTRACT**

The design and optimization of comfortable decision support systems becomes more and more important. One disadvantage of many complex systems is that they often consist of a large amount of heterogeneous single applications that are inefficiently integrated into the overall process. This happens as such processes tend to grow over time, caused by an increase of complexity and supplementary demands by users for further functionalities, which leads to demands of new applications that are added to the system and need not always be compatible to the legacy applications. This results in process inefficiencies such as breakings in the media chain, high coordination effort, redundancy and an inefficient handling of information as the processing time increases. In case of threat on a critical infrastructure element, a fast and flexible acquisition, processing, and allocation of information are crucial. Flexibility, fast adaptability, and high process efficiency are central characteristics of a Service Oriented Architecture (SOA) which qualifies it to be used in the context of OR analysis in order to protect optimally the critical infrastructure.

This contribution gives an introduction in SOA as well as an overview of an integration of SOA-elements within the analysis of complex critical infrastructures. We combine an approach from an operational point of view together within a service-orientated framework within such a complex decision support process of an OR/MS-analyst.

**1. Introduction**

**Critical Infrastructures as Complex Systems within an Uncertain Environment**

Critical infrastructures are vital elements on which our daily live and society are based on, wherefore it is of great importance to pay a special attention to the protection of these elements.

The following sectors can be identified as being critical infrastructure elements<sup>1</sup>: Banking and Finance; Chemical Industry; Commercial Facilities; Commercial Nuclear Reactors, Materials, and Waste; Dams; Defence Industrial Base; Drinking Water and Wastewater Treatment Systems; Emergency Services; Energy; Food and Agriculture; Government Facilities; Information Technology; National Monuments and Icons; Postal and Shipping; Public Health and Healthcare; Telecommunications; and Transportation Systems. Break-downs or disturbances of such critical systems as a result of e.g. war, disaster, civil unrest, vandalism, or sabotage, may cause severe damage in the supply of a wide part of users linked to these systems and can have severe consequences to vital functions of the society.

---

<sup>1</sup> George Mason University, "What is CIP", School of Law, December 2006, <http://cipp.gmu.edu/cip/>, accessed 30 March 2008

A definition is given in the “Patriot Act 2001 of the U.S.A” that describes critical infrastructures as<sup>2</sup>:

*"systems and assets, whether physical or virtual, so vital [...] that the incapacity or destruction of such systems and assets would have a debilitation impact on security, national economic security, national public health or safety, or any combination of those matters."*

Further definitions emphasize the interrelationship of the critical infrastructure elements<sup>3</sup>:

*"Critical infrastructures are the complex and highly interdependent systems, networks, and assets that provide the services essential in our daily life."*

Thus, certain sections of critical infrastructure elements depend on each other and threats or risks that concern the one can influence the other. It is obvious that classical approaches from Operational Analysis should be combined in the future with such service-orientated approaches. They might help to identify processes as well as to support a comfortable risk management.

## **2. Identification Processes and Risk Management – Vulnerability Analysis**

Hence, methods and processes for early-warning- or precautionary-, emergency planning-, information-exchange/distribution-, and recovery systems have to be developed to increase the robustness of such infrastructures. The protection of critical infrastructure elements requires the capability to identify and monitor these elements in a first step. During the monitoring phase there should be established the ability to analyse whether these elements of critical infrastructure are under attack or in danger caused to natural influences.

The identification process should be linked to a risk management process, to determine e.g. the vulnerability of certain infrastructure elements and to develop special protection plans. The Department of Defence (DoD) of the U.S.A, which is the responsible authority in the protection of the national sectors: Financial Services; Transportation; Public Works; Global Information Grid Command Control; Intelligence Surveillance, and Reconnaissance; Health Affairs; Personnel; Space; Logistics; and Defence Industrial Base, has developed a “Critical Infrastructure Protection Lifecycle” (CIP) that details the above statements and consists of the following six phases<sup>4</sup>:

- Analysis and Assessment;
- Remediation;
- Indications and Warnings;
- Mitigation;
- Incident Response; and
- Reconstitution.

---

<sup>2</sup> “USA PATRIOT ACT OF 2001”, October 2001, [http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107\\_cong\\_public\\_laws&docid=f:publ056.107.pdf](http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107.pdf), accessed 30 March 2008

<sup>3</sup> George Mason University, “What is CIP”, School of Law, December 2006, <http://cipp.gmu.edu/cip/>, accessed 30 March 2008

<sup>4</sup> Department of Defense, “The Department of Defense Critical Infrastructure Protection (CIP) Plan”, November 1998, <http://www.fas.org/irp/offdocs/pdd/DOD-CIP-Plan.htm>, accessed 30 March 2008

The Analysis and Assessment phase is the crucial part of the CIP life cycle. The identification of the vulnerability and the characteristics of critical elements such as their interrelationship to other elements are derived in this phase. During the Remediation phase, precautionary actions are taken on the base of the Analysis phase in order to fix identified vulnerabilities of the regarded element. The task of the Indications and Warnings phase focuses on the monitoring of the critical infrastructure element in order to reveal possible threats or hazards (identification) and to inform the owners or authorities linked to the element about the potential danger (warning). The Mitigation phase manages the actions that are taken in response to the analysed indications and warnings of the previous phase in order to minimize the overall threat or damage of the critical infrastructure. The Incident Response phase takes place after the occurrence of an infrastructural event that threatens the functionality of a critical infrastructure, and tries to eliminate the cause or source of this event. The final Reconstitution phase comes into action when an infrastructural event had damaged the functionality and capability of a critical infrastructure and comprises actions to recover it.

### **3. Integration of IT-based Systems (Metrics, Methods and Tools)**

The usage of IT-based Systems in order to accommodate the demand on information that is needed to achieve a sufficient situational awareness –within an Operational Analytic Approach- at the particular phases is advised. One disadvantage of many systems that are in use to support the CIP lifecycle is that they often consist of a large amount of heterogeneous single applications that are inefficiently integrated into the overall process. This happens as such processes tend to grow over time, caused by an increase of complexity and supplementary demands by users for further functionalities, which leads to demands of new applications that are added to the system and need not always be compatible to the legacy applications. This results in process inefficiencies such as breakings in the media chain, high coordination effort, redundancy and an inefficient handling of information as the processing time increases. In case of threat on a critical infrastructure element, a fast and flexible acquisition, processing, and allocation of information are crucial. Flexibility, fast adaptability, and high process efficiency are central characteristics of a Service Oriented Architecture (SOA) which qualifies it to be used in the context of the protection of critical infrastructure. Although it is difficult to define the history of Service Oriented Architecture in terms of when it was created and who founded it, SOA's history can be defined in terms of the impact it has had on industry practices and thinking. In the early days of functional programming, data and functionality were strictly separated.

The next step was merging data and functionality into encapsulated, reusable object implementations (object orientation). This worked particularly well for large, monolithic applications, such as complex graphical user interfaces.

### **4. SOA (Service Orientated Architecture)**

In the middle of the 1990s, people started to apply the concepts of object orientation to distributed systems. CORBA and a number of other standards for distributed object computing emerged. The limitations of this approach became clear when applying distributed object technology in large-scale projects. As a result, Service Oriented Architectures emerged, with supporting technology platforms such as XML Web services. Service Oriented Architectures evolved of past platforms, preserving successful characteristics of traditional architectures, and bringing with it distinct principles that foster service-orientation in support of a service-oriented enterprise. The roots of service-orientation can be found in three different areas.

The first area is concerned with Programming Paradigms: functional decomposition (COBOL, PASCAL), modularization and component programming (ADA, Visual Basic, Prolog), object-oriented programming (SIMULA, C++, Java) and service oriented computing. The second aspect involves Distribution Technology: mainframe computing, Remote Procedure Call (RPC), Distributed Component Object Model (DCOM), Common Object Request Broker Architecture (CORBA), Enterprise Java Beans (EJB). Another important area is represented by Business Computing : SAP (Systems, Applications and Products in Data Processing) introduced R/2(1981), the first business-computing platform that enabled enterprise-wide real time processing of financial data and resource planning information. Complex enterprise applications emerged in the past years: Enterprise Resources Planning (ERP), Supply Chain Management (SCM), Customer Relationship Management (CRM).<sup>5</sup>

Service-Oriented Architecture is both: a design concept and architecture. The design concept in SOA is about designing applications/systems that have well defined self-describing access interfaces, having services composed into business processes. The architecture is about having simple mechanisms to use these access-interfaces for integration purposes.<sup>6</sup>

A formal definition of Service Oriented Architecture is given by Thomas Erl in his book “Service-Oriented Architecture: Concepts, Technology, and Design”, stating that:

*“A contemporary SOA represents an open, agile, extensible, federated, composable architecture comprised of autonomous, QoS-capable, vendor diverse, interoperable, discoverable, and potentially reusable services, implemented as Web services.”<sup>7</sup>*

Although Service Oriented Architecture solutions are technology independent, the broad acceptance of the web service design model made the web-based implementation of an SOA to a standard solution. Among technologies like web services, XML (Extended Markup Language) is used to send and receive data in a standardized format, and HTTP (Hypertext Transfer Protocol) is used as communication protocol. Furthermore, supplementary technologies have become de facto standards. The most important are briefly described in the following. Primarily a communication protocol, Simple Object Access Protocol (SOAP) which is platform and language independent, allows the communication between processes. Based on XML, it is used for describing and sending messages. The Web Services Description Language (WSDL) describes the interface to the web service using XML. It indicates where the service is located and what operations are provided for use. The Universal Description, Discovery and Integration (UDDI) directory serves as a place where the registration and search for web services are managed. Many software solutions that support SOA implementations have been developed and a large amount is available as open source (J2EE, Fuse, WebSphere).

The main motivation for creating a SOA is the desire to increase agility of IT systems. In addition, SOAs offer benefits at several levels, ranging from a reduction of technology dependence to a simplification of the development process to an increase in flexibility and reusability of the system’s infrastructure.

---

<sup>5</sup> Dirk Krafzig, Karl Banke, *Enterprise SOA: Service-Oriented Architecture Best Practices*(Prentice Hall PTR, 2004), Ch 2.2-2.4

<sup>6</sup> Juric, Loganathan, Sarang, Jennings, *SOA Approach to Integration*(Birmingham: Packt Publishing, 2007), 57

<sup>7</sup> Thomas Erl, *Service-Oriented Architecture: Concepts, Technology, and Design*(Prentice Hall PTR, 2005), Ch 3.2.11



The ultimate goal of the additional reusability and flexibility provided by a SOA is the agile system platform, in which all processes and services are completely flexible and can be rapidly created, configured, and rearranged as required by experts without the need for technical staff. This facilitates a superior reaction time. Another motivating factor is the potential of efficiency, balancing the complexity that threatens a certain element of critical infrastructure on different levels. Identifying the following elements of complexity: technology, processes, functionality, integration, maintenance, the simplicity is achieved through: decomposition, appropriate granularity, decoupling from technology, reuse and documentation. Cost Savings can be obtained through reduced project costs, reduced maintenance costs, and the development of future proof solutions. Further benefit is contributed through the reuse of existing code that significantly reduces the risk of failure in following projects. The service itself can be used in different technological contexts that guarantee a protection of investment.<sup>8</sup>

## **5. Risk Assessment and Management: SOA and CRISYS (Critical Infrastructure and System Analysis) - Complex Scenarios**

It is possible to create a new service simply by choreographing existing building blocks. SOA allows for a more efficient development process and a high degree of modularity, which in turn makes it possible to decouple the development process. The overhead of project management is significantly reduced. Using SOA facilitates independence from technology; choosing the best of breed products and combining them as required by the particular application field, helps to shift the attention from technological issues to questions of service functionality and service design. SOA might be an excellent technique to be integrated in a complex system analytic process to protect critical infrastructures.

In the following, the focus will be put on a special scenario and the description of a system that is extremely valuable in the protection of critical infrastructures. The advantages of a SOA-based development of the system will become obvious. Imagining the potential threat of a terrorist vehicle carrying a hazardous load possibly heading towards an identified element of critical infrastructure, demands for a system that reports the current position of this vehicle to the authorities capable of escalating this potential threat. A system that accommodates this demand is referred to as a tracking and monitoring system. This system is vital for several phases mentioned in the first part of this paper: Indications and Warning phase that implies monitoring of the critical infrastructure elements to reveal possible threats and to inform authorities about the potential danger:

- The Mitigation phase in which the tracking system can help to minimize the overall threat on the critical infrastructure.

Even more, the Incident Response phase which tries to eliminate the cause or source of the event (which in this case is the terrorist vehicle) could not be carried out without a tracking and monitoring system. A vehicle tracking system is an electronic device installed in a vehicle in order to enable the owner or a third party to track the vehicle's location. Most modern vehicle tracking systems use Global Positioning System (GPS) modules for an accurate location of the vehicle. Many systems also combine a communications component such as cellular or satellite transmitters to communicate the vehicle's location to a remote user. Vehicle information can be viewed on electronic maps via the Internet or specialized software. Current vehicle tracking systems have their roots in the shipping industry.

---

<sup>8</sup> Dirk Krafzig, Karl Banke, *Enterprise SOA: Service-Oriented Architecture Best Practices*(Prentice Hall PTR, 2004), Ch 11.1

Corporations with large fleets required some sort of system to determine where each vehicle or vessel is at any given time. There exist several types of vehicle tracking devices. Typically they are classified as passive and active. Passive devices store GPS location, speed, heading and sometimes a trigger event such as key on/off, door open/closed. Once the vehicle returns to a predetermined point, the device is removed and the data downloaded to a computer for evaluation. Passive systems include an auto download type that transfer data via wireless download. Active devices also collect the same information but usually transmit the data in real-time via cellular or satellite networks to a computer or data center for evaluation. In the following, the focus will be put on active systems<sup>9</sup>. A vehicle tracking system can efficiently monitor and, equipped with the relevant devices, even control vehicles. Technologies used in this process linked with means of wireless communication are essential to the system determining the vehicle location. It is required to have a technique to handle the huge amount of spatial data entailed in a digital road map in order to trace the accurate position within a reasonable time. The GIS (Geographic Information System) and GPS (Global Positioning System) technology have brought some breakthrough in the area of transportation monitoring.

One of the most useful applications<sup>10</sup> is a vehicle tracking and monitoring system to determine and trace the position of the mobile object (automobile, vessel, aircraft, etc.). Especially, the land vehicle tracking system locates vehicles using GPS satellites, GPS receivers and auxiliary equipments, and displays the geographical coordinate of the vehicle position on a digital road map of the monitoring system. GPS is a navigation support system developed originally for military purpose. Recently, GPS technology is widely spread and used in many applications, since its C/A (Coarse Acquisition) code is freely available to civilians. According to the near live report of the 2d Space Operations Squadron (2 SOPS) at Schriever AFB, CO who operates the GPS system, there are currently 28 satellites in activity. At least four of them are observable from any place in the globe. Unlike one might think GPS satellites are not geostationary (except the SBAS satellites) as they orbit at about 20,000 kms of altitude.

## **6. Monitoring and Tracking – Role of Metrics, Methods and Tools (Operations Research/Management Science)**

This means that depending on your position, at certain times, the "sky" will be unfavourable (poor alignment and elevation of satellites) and it will be difficult for a GPS receiver to have a good communication with the satellites. GPS satellites transmit two low power radio signals, designated L1 and L2. Civilian GPS uses the L1 frequency of 1575.42 MHz in the UHF band<sup>11</sup>. The signals travel by line of sight, meaning they will pass through clouds, glass and plastic but will not go through most solid objects such as buildings and mountains. A GPS signal contains three different bits of information — a pseudorandom code, ephemeris data and almanac data. The pseudorandom code is simply an I.D. code that identifies which satellite is transmitting information<sup>12</sup>.

---

<sup>9</sup> Parkinson, B.W. ,*Global Positioning System: Theory and Applications* (1996) ch 1

<sup>10</sup> Satellite Navigation & Positioning Laboratory (SNAP Lab) , „Principles and Practice of GPS Surveying“, [http://www.gmat.unsw.edu.au/snap/gps/gps\\_survey/chap12/1233.htm](http://www.gmat.unsw.edu.au/snap/gps/gps_survey/chap12/1233.htm) , accessed 30 March 2008

<sup>11</sup> Satellite Navigation & Positioning Laboratory (SNAP Lab) , „Principles and Practice of GPS Surveying“, [http://www.gmat.unsw.edu.au/snap/gps/gps\\_survey/chap3/311.htm](http://www.gmat.unsw.edu.au/snap/gps/gps_survey/chap3/311.htm) , accessed 30 March 2008

<sup>12</sup> Satellite Navigation & Positioning Laboratory (SNAP Lab) , „Principles and Practice of GPS Surveying“, [http://www.gmat.unsw.edu.au/snap/gps/gps\\_survey/chap3/312.htm](http://www.gmat.unsw.edu.au/snap/gps/gps_survey/chap3/312.htm) , accessed 30 March 2008

Ephemeris data tells the GPS receiver where each GPS satellite should be at any time throughout the day. Each satellite transmits ephemeris data showing the orbital information for that satellite and for every other satellite in the system. Almanac data, which is constantly transmitted by each satellite, contains important information about the status of the satellite (healthy or unhealthy), current date and time. This part of the signal is essential for determining a position. A GPS receiver accepts the signals involving the satellite's clock and orbit information of each one of the seen satellites and calculates the difference between the receiver clock at the signal's reception time and the satellite clock at its transmission time. The time difference derives a distance (usually called pseudo range) from the receiver to each one of the satellites and then the location of each satellite can be elicited from its orbit information. Finally, the location of the receiver is computed by the triangular measurement using the resulting positions of those satellites<sup>13</sup>.

The vehicle tracking system needs to be channelized by a wireless communication link from the receiver of the vehicle to the monitoring station. Beyond this kind of immediate demand, the advent of wireless era accelerates the nationwide construction of various wireless networks. Currently, a conventional private network, a TRS (Trunked Radio System) network, a cellular network, a satellite network and a data packet network may be a candidate for the application:

- All concepts explained above could be bound together within an Operational Analysis in order to obtain a perspective view of the entire monitoring system.

Recalling the previous example of the potential threat through a terrorist vehicle carrying a hazardous load (e.g. chemicals, explosives, radioactive substances, etc.), possibly heading towards an identified element of critical infrastructure, and the hereby arising demand for a system that is able to track its position, the described tracking and monitoring system is advised. Implementing the needed devices at the target vehicle (tagging) – possibly during a stop at a gas station or any other scenario – or making use of already implemented sensors (like e.g. already installed GPS-modules in rental cars) makes it possible to apply a tracking and monitoring system.

A very important part of the entire system consists in a collection of software programs able to ensure an efficient communication between a GPS receiver and a processing unit. All information received should be analyzed by experts in different domains: communications, radioactive materials, national security, situational awareness, chemical weapons, etc. One or more teams placed in different locations across the entire area (or all over the world) are needed.

Collaboration between different teams is usually ensured by different software tools. Also a secure infrastructure is needed to prevent unauthorized access. Virtual Private Networks are used and particular communication protocols are implemented in order to ensure privacy. All software tools involved should communicate with each other, and the integration of new functionalities must be achieved in a simple, flexible and efficient way. Agility, modularity, ease of integration, technology independence and reusability should be the main characteristics of the entire system's architecture.

SOA natively supports these characteristics and much more, allowing a system in which processes and services are completely flexible and can be rapidly created, configured,

---

<sup>13</sup> Aidala, V. J. and Hammel, S. E., "Observability Requirements for Three-Dimensional Tracking Via Angle Measurements," *IEEE Transactions on Aerospace and Electronic Systems*, AES-21, 2 (Mar. 1985): 200-207.

rearranged, and exchanged as required. These features of a SOA accommodate the demands for an efficient information handling and reaction time in situations general OR/MS applications as well as the threat on critical infrastructure elements.

## 7. Summary

This contribution combines a traditional operational approach within the analysis of critical infrastructures with a Service Oriented Architecture (SOA)-framework. An introduction into SOA and its characteristics is presented. Advantages of flexibility, fast adaptability, and high process efficiency are central characteristics of a Service Oriented Architecture which qualifies it to be used in the context of the analysis and protection of critical infrastructures. As critical infrastructure security will be an important task in the future there might be a need to combine pure analytic approaches with software-engineering capabilities. The integration of SOA into Operations Management and Operational Analysis will become more and more important in the near future. First possible applications and results within such an OR/MS-process to support intelligent decision support systems are illustrated.

## 8. Acknowledgement

The authors want to thank Alex Bordetsky for stimulating discussions and all his help to be integrated in the Maritime Interdiction Operation (MIO)-experiments series.

## REFERENCES

- Aidala, V. J and Hammel, S. E , "Observability Requirements for Three-Dimensional Tracking Via Angle Measurements," *IEEE Transactions on Aerospace and Electronic Systems*, AES-21, 2 (Mar. 1985): 200-207.
- Dirk Krafzig, Karl Banke, *Enterprise SOA: Service-Oriented Architecture Best Practices* (Prentice Hall PTR, 2004), Ch 2.2-2.4
- Dirk Krafzig, Karl Banke, *Enterprise SOA: Service-Oriented Architecture Best Practices* (Prentice Hall PTR, 2004), Ch 11.1
- Juric, Loganathan, Sarang, Jennings, *SOA Approach to Integration* (Birmingham: Packt Publishing, 2007), 57
- Parkinson, B.W. ,*Global Positioning System: Theory and Applications* (1996) ch 1
- Thomas Erl, *Service-Oriented Architecture: Concepts, Technology, and Design* (Prentice Hall PTR, 2005), Ch 3.2.11
- Department of Defense, "The Department of Defense Critical Infrastructure Protection (CIP) Plan", November 1998, <http://www.fas.org/irp/offdocs/pdd/DOD-CIP-Plan.htm>, accessed 30 March 2008
- George Mason University, "What is CIP", School of Law, December 2006, <http://cipp.gmu.edu/cip/>, accessed 30 March 2008

Satellite Navigation & Positioning Laboratory (SNAP Lab), „Principles and Practice of GPS Surveying“, [http://www.gmat.unsw.edu.au/snap/gps/gps\\_survey/chap12/1233.htm](http://www.gmat.unsw.edu.au/snap/gps/gps_survey/chap12/1233.htm) , accessed 30 March 2008

Satellite Navigation & Positioning Laboratory (SNAP Lab), „Principles and Practice of GPS Surveying“, [http://www.gmat.unsw.edu.au/snap/gps/gps\\_survey/chap3/311.htm](http://www.gmat.unsw.edu.au/snap/gps/gps_survey/chap3/311.htm) , accessed 30 March 2008

Satellite Navigation & Positioning Laboratory (SNAP Lab), „Principles and Practice of GPS Surveying“, [http://www.gmat.unsw.edu.au/snap/gps/gps\\_survey/chap3/312.htm](http://www.gmat.unsw.edu.au/snap/gps/gps_survey/chap3/312.htm) , accessed 30 March 2008

“USA PATRIOT ACT OF 2001”, October 2001, [http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107\\_cong\\_public\\_laws&docid=f:publ056.107.pdf](http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107.pdf), accessed 30 March 2008



A significant step in the direction of understanding and anticipating developments in our national security challenges has been the focus on irregular warfare (IW) and its associated socio-political landscape. Terrorist organizations do not exist in a political or social vacuum. While nation-level politics in the specific areas affected by terrorist networks and insurgents are important, all terrorist recruiting is local and thus is greatly affected by local conditions. If we are to design effective, affordable, and sustainable interventions and policies, we must understand how terrorist networks function within local and broader systems in social, political, and economic domains.

From anthropological studies, we know that local populations in the Middle East tend to exhibit fractious tribal and religious affiliations. Tribal groups may unite or divide as situation on the ground dictates, in a fluid and rapidly evolving network of alliances and rivalries. When attacks by insurgents or coalition forces result in civilian deaths and injuries, emotional effects of these events radiate through the population along these complex network structures, resulting in sharp, unstable changes in support for the insurgency in a local population.

By modeling how members of the population make a choice between joining or supporting the insurgency, joining the counter-insurgency, or remaining unaffiliated, we attempt to understand the dynamics of the region, and provide a tool for policy experimentation and training. Our prototype model demonstrates emergence of ethnic cleansing and inter-tribe violence sparked purely by external factors.

Can a successful policy quell the violence? Is there a solution to the crisis? We cannot give definitive answers, but we hope to contribute to the body of understanding and an eventual positive result.





# Introduction to the Terrorism Risk Assessment and Management (TRAM) Methodology

---

**Chel Stromgren**

**Kevin A. Ryan**

Science Applications International Corporation

1710 SAIC Drive

McLean, VA 22102, U.S.A.

State and local jurisdiction are increasingly relying on risk-based management approaches to allocate resources for security and emergency planning. Recognizing the needs of these jurisdictions to identify and prepare for potential terrorism risks, Science Applications International Corporation (SAIC), in partnership with the U.S. Department of Homeland Security (DHS), National Preparedness Directorate (NPD), developed the Terrorism Risk Assessment and Management (TRAM) methodology to help local jurisdictions implement a robust continuous risk management capability. The TRAM compares the relative risk of acts of terrorism against critical assets owned or operated by organizations and identifies and prioritizes enhancements in security, emergency response, and recovery that could be implemented to reduce those risks.

## 1. Origin of TRAM Methodology

The TRAM Methodology was originally developed, applied, and validated by DHS in conjunction with the Port Authority of New York and New Jersey (PANYNJ) in the period following 9/11. Following the attacks on the World Trade Center Towers, PANYNJ recognized the need to implement robust risk-based processes to evaluate options for improvements in security, response, and recovery, and to allocate resources towards solutions that would provide the greatest return on investment, in the form of risk reduction. Therefore, PANYNJ sought technical assistance from DHS to develop a continuous risk management capability for critical infrastructure protection that could be implemented at the working jurisdictional level. In response to the Port Authorities' needs, DHS/PANYNJ/SAIC developed TRAM. Following the successful development of this capability for PANYNJ, DHS recognized a need across a multitude of state and local agencies for a similar capability and decided to make the methodology and toolset available to other jurisdictions.

## 2. Overview of the Continuous Risk Management Process

Risk management is a process that relies on risk-based metrics to identify hazards that pose a potential loss to a jurisdiction and to evaluate and select mitigation strategies to reduce those potential losses. A robust risk management process involves three key elements: continuous risk assessment, historical risk tracking, and risk mitigation.

The core of the risk management process is continuous risk assessment. Accurate prediction of risk, based on the likelihood and expected consequence of events, forms the basis for all risk management activities. A risk assessment allows jurisdictions to identify those hazards that are most significant to the jurisdiction and to prioritize assets for risk mitigation. Risk assessment should be conducted in a continuous manner. As risk drivers change over time as a result of the implementation of new mitigation measures or through changes in the threat profile or changes to the criticality of assets, the risk profile of the jurisdiction should be updated.

Historical risk tracking is a process of looking backwards in time in order to evaluate how effective a jurisdiction has been at reducing risk and making effective investments. By comparing the risk profile of the jurisdiction over time, it is possible to see by how much the risk of various events has changed. It is also possible to analyze those changes and to determine what variations occurred in the jurisdiction that resulted in a change in the level of risk. It is possible to analyze specific risk mitigation projects that have been implemented and to compare the effectiveness of those investments.

Finally, risk mitigation is the process of looking forward in time to evaluate future risk mitigation solutions. This component of the risk management process allows jurisdictions to evaluate potential mitigation projects, in the form of physical security, operational security, response, or recovery improvements, to measure the risk reduction that would result from the implementation of those projects, and to compare the risk reduction to the estimated cost, selecting those projects that would result in the greatest return on investment.

The TRAM methodology that emerged from the initial DHS/PANYNJ/SAIC partnership was designed to meet all three of these objectives. First, it implements a structured risk-based analytical process to approach analysis. Second, TRAM established processes and metrics for continuous risk tracking. Finally, TRAM can be used to support investment decision making by clearly articulating to decision makers the expected ROI of investments. The final analysis from TRAM communicates and ranks possible security, response, and recovery investments in terms risk reduction achieved per dollar invested.

TRAM is provided to local jurisdictions as a software tool that allows organizations to perform risk management activities as part of their normal security and emergency management practices.

Reflecting the breakdown of risk management activities, the application of the TRAM methodology is divided three distinct component phases. The first main component, the Comprehensive Risk Assessment, involves the application of a framework to evaluate the relative risk of attacks by terrorist groups against an organization's critical assets. This framework is presented in Figure 1, and involves an evaluation of Criticality, Threat, Vulnerability, Response & Recovery, and Impact. Scenarios are developed and evaluated within this framework to allow comparison of these factors across dissimilar assets with varying missions.

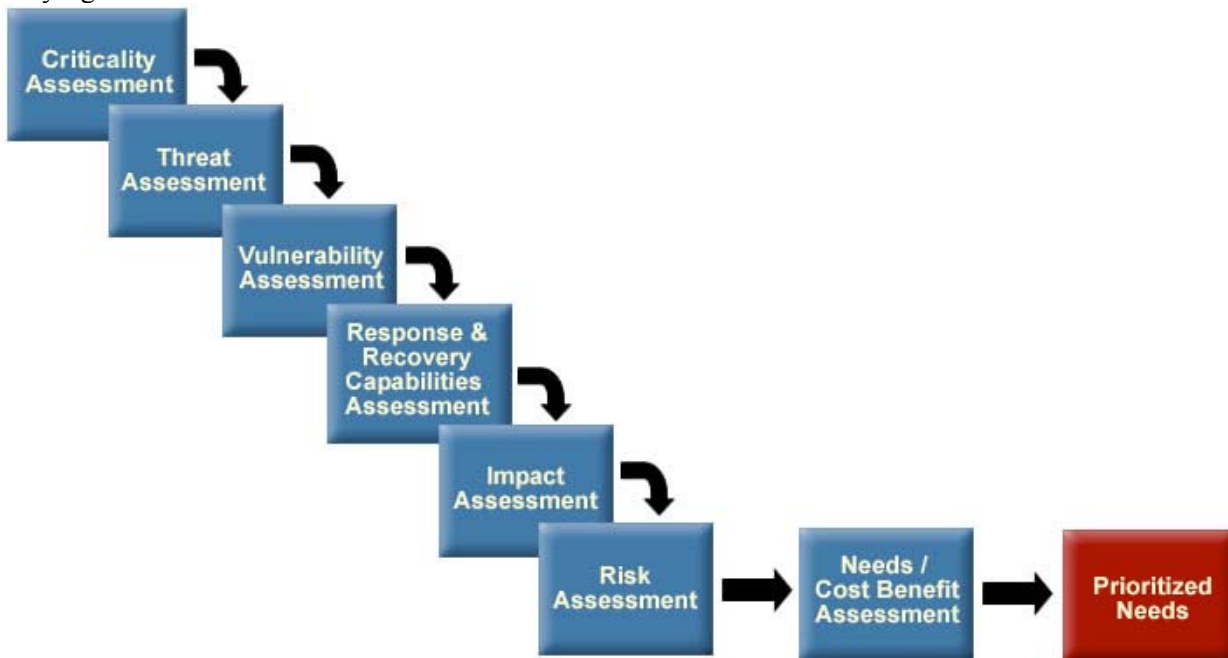


Figure 1: The 8 Steps of the TRAM Methodology's Risk Assessment Process

### 3. Risk Assessment Process → Criticality Assessment

The TRAM Risk Assessment Process begins with a comprehensive Criticality assessment. Criticality describes the overall importance of an asset to the jurisdiction, to the region, and to the nation. As part of the TRAM process, workshops are typically conducted to gather input from representatives of the organization regarding the criticality of assets. The first step in this assessment is to develop a comprehensive list of assets within the organization. Assets having similar Threats, Criticalities, Vulnerabilities, and Risks and are typically grouped as representative asset types. After a list of assets has been developed, Critical Asset Factors (CAFs) are established. CAFs represent the goals and mission of the organization and are used to quantify the relative importance of assets using a multi-attribute scale. Typical CAFs include: Potential for Casualties, Potential of Business Continuity Loss, Potential National Strategic Importance, Potential Economic Impact, Potential Loss of Emergency Response function, Potential Replacement Cost, and Potential Environmental Impact. The established CAFs are then compared and rated on their relative importance to the organization’s mission. Ratings are made on a scale of one (1) to five (5), with “1” being least important to the overall mission and “5” being of maximum importance.



Figure 2: Criticality diagram.

Once the CAFs are defined and rated, they are applied to each asset. For each CAF, an asset applicability rating of zero (0) to ten (10) is assigned, indicating the extent to which the factor applies to each asset. In using this approach, some agreement is necessary on what constitutes the “upper-bound” of each CAF – that is, when assigning a rating of 0 to 10, if “0” means the factor does

not apply to the asset, what does a “10” mean? Representatives of the jurisdiction must collectively develop “upper-bound” criteria for each CAF.

Representatives of the jurisdiction must collectively

Finally, for each asset, each CAF rating (1 – 5) is multiplied by the asset applicability for that CAF (0 – 10) and the results are summed for all factors. The resultant total is the Criticality of that asset. This number represents a quantified measurement of the total potential impact to the organization’s mission if that asset were completely destroyed. Once asset criticality ratings are obtained by the organization, the asset list is sorted in descending order with the highest ratings (most critical assets) at the top of the list. This provides the jurisdiction a clear direction on the assets that require attention when considering Risk. Figure 3 displays sample criticality results.

		Death / Injury	Economic Impact	National Defense	Environmental Impact	Symbolic Effect	Replacement Cost	
#	CAF Value →	5	5	3	2	2	2	190
	Asset Name							Total
1	Asset A	10	4	0	2	6	10	106
2	Asset B	10	4	0	2	6	5	96
3	Asset C	1	10	1	1	1	10	82
4	Asset D	1	10	1	1	1	10	82
5	Asset E	4	8	2	1	1	6	82

Figure 3: Sample criticality results.

### 4. Risk Assessment Process → Threat Assessment

The TRAM risk assessment is scenario based. To define an applicable set of scenarios for the risk assessment, each scenario is broken into the asset to be attacked and threat of attack on each asset. Threat describes the likelihood of a specific type of event occurring or being directed at a specific asset. The Threat Assessment component of the TRAM methodology is used to identify possible attacks against assets previously determined through the Criticality Assessment and to quantify the plausibility and

severity of those attacks. The end result of the Threat Assessment is the development of a Threat Rating for each attack scenario devised for the critical assets.

In basic terms, Threat can be broken down into two components: the Capability of a terrorist to execute and attack, and the Intent of that terrorist. “Capability” captures the general likelihood that a terrorist organization would execute a given attack based on the complexity of obtaining a weapon and executing the attack. “Intent” describes the likelihood that a terrorist organization would execute a given attack against a specific asset based on the asset’s target attractiveness and level of deterrence. The process for calculating threat is described in Figure 4.

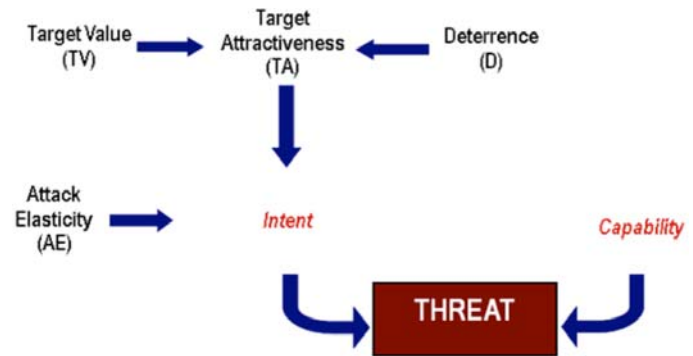


Figure 4: TRAM process for determining Threat.

To determine a terrorist’s capability for executing an attack, a set of potential attack types are developed. The most common attacks assessed in the TRAM methodology are: Small Conventional Explosive (SCE), Large Conventional Explosive (LCE), Chemical Weapons, Radiological Weapons, and Biological Weapons. Attack Ratings are based on the likelihood that a terrorist possesses the capability to carry out an attack and is prepared to use that capability against the organization’s assets.

Attack Likelihood Ratings represent the capability of adversaries and are developed for each Attack Type by a group of threat experts and organizational representatives with specific local knowledge. For each Attack Type, the likelihood of use is rated on a relative scale from highly unlikely (0) to highly likely (10). It is important to note that the Attack Likelihood rating does not measure the likelihood of an attack against a specific target, but rather measures the general likelihood that such an attack could occur somewhere within the jurisdiction or organization. To evaluate the likelihood of an attack on a specific target the intent on the adversaries must also be evaluated.

The first step in determining intent is to evaluate the Target Attractiveness of each asset from a terrorist’s perspective based on two drivers: Target Value and Deterrence. Target Value represents the goals of the terrorist in attacking a target, and is rated on a scale of 0-10. Deterrence takes into account the features of an asset that would make that asset less attractive as a target for a terrorist and is also rated on a 0-10 scale. A low Deterrence rating (0) indicates that the asset is not attractive, or that the perception of the adversary is that offensive action would be futile. A high Deterrence rating (10) indicates that the asset is attractive as a target, or indicates that the perception of the adversary is that success of the attack is certain.

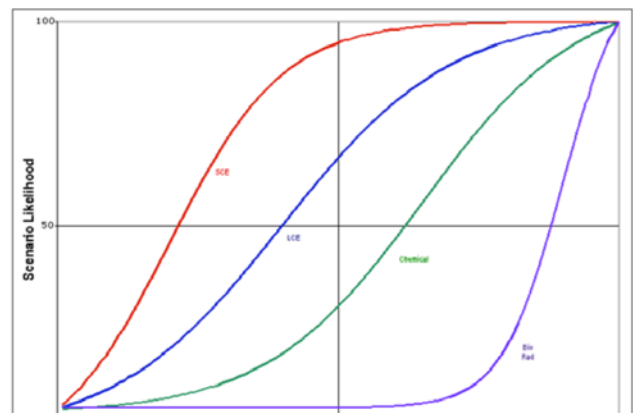


Figure 5: Attack Elasticity is used to determine scenario likelihood, based on the attractiveness of the target, and the type of weapon used in the attack.

Scenario Likelihood measures the relative likelihood that a specific scenario would be carried out against a particular target and is a function of Target Attractiveness and an

Scenario#	Asset	Attack Type	Attack Likelihood	Scenario Likelihood	Threat
1	Asset A	LCE land	6	41.2	247.5
2	Asset A	LCE water	5	41.2	206.2
3					
4					
5					
6	Asset A	SCE Land	10	86.7	866.9
7	Asset B	LCE water	5	18.4	92.2
8	Asset C	LCE water	5	18.4	92.2
9	Asset C	LCE land	6	78.9	473.1
10	Asset C	LCE water	5	78.9	394.3
11	Asset C	SCE land	10	97.8	978.2
12	Asset C	CHEM Bldg	2	44.4	88.8
13	Asset D	LCE land	6	41.6	249.5
14	Asset D	LCE water	5	41.6	207.9

Figure 6: Sample Threat calculations.

Attack Elasticity parameter. The Scenario Likelihood rating reflects the intentions of the terrorist with regard to the type of attack under consideration. For simple Attack Types or for weapons that are easier to obtain, a relatively low Target Attractiveness might be acceptable to the terrorist. For a more complex attack or for weapons that are more difficult to obtain and/or deliver, terrorists would likely demand a greater level of Target Attractiveness. Figure 5 shows the relationship between Scenario Likelihood and Target Attractiveness for different attack types. The rate at which the Scenario Likelihood decreases, in relation to the Target Attractiveness, is dependent on the shape of the curve for each Attack Type. The shape is defined by the Attack Elasticity parameter. The Attack Elasticity parameter is a measure of the sensitivity of the Attack Likelihood to the Target Attractiveness of that particular asset. The rating specifies the horizontal position of the scenario likelihood curve. Once Attack Elasticity values for different attack types are established, the Scenario Likelihood values for each scenario can be determined. Assets with a greater Target Attractiveness will have a greater Scenario Likelihood for a given Attack Type.

### **Scenario Discussion/Development**

Once intent and capability have been determined, the next step in the Threat Assessment is to select a set of plausible attack scenarios for each asset. Each selected attack scenario consists of a specific Attack Type being applied against a specific asset. Scenarios are selected based on the Scenario Likelihood rating and the plausibility of a particular Attack Type (e.g., scenarios using chemical or biological agents to attack an open air structure such as a bridge are disregarded). Other criteria used to develop scenarios include: High Scenario Likelihood, High perceived Vulnerability, High Criticality, and specific threats to asset, History of attacks on assets of similar type or function. Figure 6 displays sample threat calculations and shows that the Threat Rating is the product of the Attack Likelihood and the Scenario Likelihood. This Threat Rating represents the relative likelihood of a scenario being executed by a terrorist.

## **5. Risk Assessment Process → Vulnerability Assessment**

The third component of the TRAM risk assessment is the Vulnerability Assessment. The purpose of the Vulnerability Assessment is to identify the likelihood that each of the attack scenarios selected in the Threat Assessment would be successfully executed if attempted. The objective is to evaluate the susceptibility of critical assets to a particular attack scenario. The output of this process is an overall rating of the asset's vulnerability. This rating is determined by evaluating security countermeasures that are in place to deny accessibility to an attack, evaluating the likelihood an attack would be detected, and evaluating the likelihood that a detected attack could be successfully interdicted. The attack scenarios are kept general in nature so that they take into consideration all of the potential vulnerabilities at an asset, and are not written to specifically exploit one particular vulnerability. This prevents recommendations from being limited to protecting against one particular avenue of attack on an asset. However, specific vulnerabilities are evaluated in the rating process, to ensure that identified needs address these vulnerabilities.

During the Threat Assessment, threat experts conduct site visits to assets with high criticality ratings or high perceived vulnerabilities. During these visits, participants use a checklist of security countermeasures to determine what types of countermeasures are present at each asset. Certain countermeasure types are specific to an asset while other countermeasures function across a jurisdiction. Jurisdiction-wide countermeasures are applied to every asset during the Vulnerability Assessment. Built into these checklists is a class system to rate each security countermeasure. The class system includes specific descriptions and guidelines of the capabilities that are represented by each class of security. Class ratings start at "0" which represents no capability in that area. Higher class ratings indicate increasing levels of capability and security. The Threat Experts uses these checklists to specify which countermeasures are present at each asset. Table 7 is an example of the class guidelines used for fencing systems.

The specifics of each scenario and the types of countermeasures present are used to evaluate the likelihood that the scenario would be successfully executed. This is accomplished by determining the likelihood of three vulnerability factors:

- **Access Control (L<sub>1</sub>)** What is the likelihood that access will be denied?
- **Detection Capabilities (L<sub>2</sub>)** What is the likelihood that the attack would be detected either while access is being attempted or after access is gained?
- **Interdiction Capabilities (L<sub>3</sub>)** If detected, what is the likelihood the attack will be interdicted?





LANDSIDE HARDENED VEHICLE PERIMETER AND ACCESS POINTS	EXAMPLE	Example Likelihood Reduction Ratings
<p><b>High Security (Class IV)</b> - Class IV consists of a permanent barrier, mechanical or natural, resistant up to a 15,000lb vehicle traveling at 50mph which results in vehicle penetration less than 3ft. Vehicle entrance gates must be hardened to the same standard. (DOS K12/L3). Includes appropriate personnel to man the gate/checkpoint.</p> <p><b>Guidelines:</b> Barrier could be horizontal or vertical structures constructed of various materials designed to stop the above specified weight/speed vehicle penetration.</p>		<p>→ L<sub>1</sub> = 0.8</p>
<p><b>Medium Security (Class III)</b> - Class III consists of a permanent barrier, mechanical or natural, resistant up to a 15,000lb vehicle traveling at 40mph which results in vehicle penetration less than 20ft. Vehicle entrance gates must be hardened to the same standard. (DOS K8/L2). Includes appropriate personnel to man the gate/checkpoint.</p> <p><b>Guidelines:</b> Barrier could be horizontal or vertical structures constructed of various materials designed to stop the above specified weight/speed vehicle penetration.</p>		<p>→ L<sub>1</sub> = 0.6</p>
<p><b>Intermediate Security (Class II)</b> - Class II consists of a permanent barrier, mechanical or natural, resistant up to a 15,000lb vehicle traveling at 30mph which results in vehicle penetration less than 50ft. Vehicle entrance gates must be hardened to the same standard. (DOS K4/L1). Includes appropriate personnel to man the gate/checkpoint.</p> <p><b>Guidelines:</b> Barrier could be horizontal or vertical structures constructed of various materials designed to stop the above specified weight/speed vehicle penetration.</p>		<p>→ L<sub>1</sub> = 0.4</p>
<p><b>Low Security (Class I)</b> - Class I consists of a fixed or movable barrier, mechanical or natural, designed to limit or redirect vehicular access. This barrier system will act as a deterrent to a forced vehicular penetration.</p> <p><b>Guidelines:</b> Barrier could be a concrete jersey barrier, planter, concrete jack, bollard, or barriers of similar nature.</p>		<p>→ L<sub>1</sub> = 0.1</p>

Table 7: Sample Evaluation Criteria used by Threat experts.

The TRAM tool contains a set of rating guidelines that allow analysts to produce LSA ratings for the three likelihood factors, based on the attack type and on the classes of security countermeasures that are present at the asset. These guidelines, which were developed by security and threat experts, facilitate the assessment process and provide for consistency in ratings between assets and assessments. However, all ratings are still evaluated by threat experts to ensure that the tool calculated guideline ratings are applicable to each particular asset and scenario.

The three likelihood ratings are used in an event tree process to produce the overall LSA for each attack scenario. Figure 8 illustrates an example decision tree analysis. It is assumed that an attack will be successful if not detected, or if detected and not interdicted. This avoids immeasurable and/or unpredictable externalities such as weather, faulty weapons, or attacker incompetence.

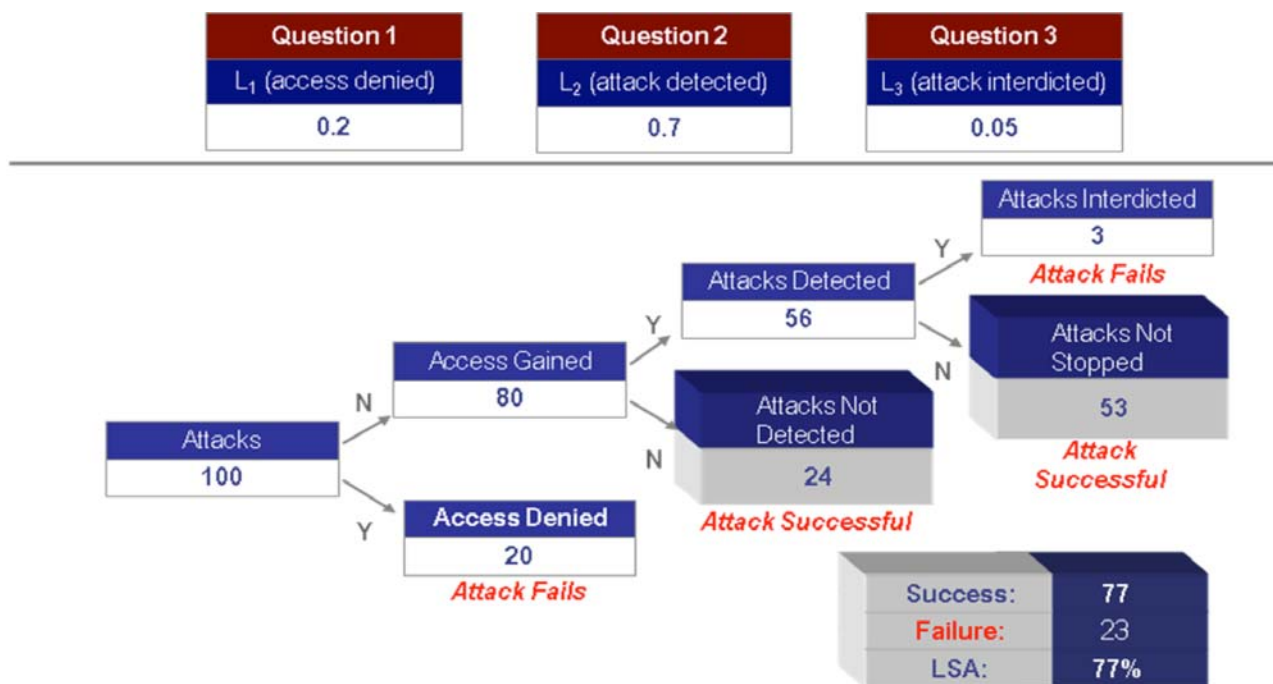


Figure 8: Event tree analysis example.

The process of evaluating the three vulnerability factors involves rating the likelihood of each on a range from 0.0 (POOR: highly vulnerable) to 1.0 (EXCELLENT: highly secure). In this example, if each of the three factors were rated at a likelihood of 0.5, it would indicate that one-half of all attacks would gain access to the target, one-half of those that gained access would be detected, and one-half of the attacks that are detected would be interdicted before they were successfully executed. The event tree uses these likelihoods to determine the total percentage of attacks that would be successful. This final value is the LSA rating, which represents the likelihood that particular attack scenario would be successfully carried out. Figure 9 shows an example set of vulnerability results.

#	Asset	Attack Type	L <sub>1</sub>	L <sub>2</sub>	L <sub>3</sub>	LSA
1	Asset A	LCE	0.00	0.32	0.12	0.96
2	Asset A	LCE water	0.00	0.14	0.10	0.99
3	Asset A	SCE Bldg	0.05	0.49	0.18	0.86
4	Asset A	SCE scuba	0.00	0.06	0.10	0.99
5	Asset A	BIO Bldg	0.05	0.32	0.14	0.91
6	Asset A	CHEM Bldg	0.05	0.46	0.14	0.89
7	Asset B	LCE water	0.00	0.17	0.10	0.98
8	Asset C	SCE Bldg	0.03	0.49	0.17	0.89
9	Asset C	SCE scuba	0.00	0.06	0.10	0.99
10	Asset C	BIO Bldg	0.03	0.33	0.12	0.94
11	Asset C	CHEM Bldg	0.03	0.46	0.12	0.92
12	Asset D	LCE water	0.00	0.06	0.10	0.99
13	Asset D	SCE Bldg	0.00	0.35	0.17	0.94
14	Asset D	BIO Bldg	0.00	0.20	0.12	0.97
15	Asset D	CHEM Bldg	0.00	0.32	0.12	0.96

Figure 9: Example of LSA ratings.

## 6. Risk Assessment Process → Response & Recovery Capabilities Assessment

The fourth component of the TRAM risk assessment involves an evaluation of the jurisdiction’s ability to respond to and recover from terrorist attacks. This assessment is unique in that it does not consider preventative measures against terrorist acts, but rather looks strictly at the organization’s ability to respond to and recover from an attack that has occurred.

The Response Assessment provides the jurisdiction and local emergency response agencies a “self-assessment” tool to identify capabilities, gaps and shortfalls across functional areas, to include: Staffing & Personnel, Training, Equipment & Systems, Planning, Exercise, Evaluation & Corrective Actions, and Organization & Leadership. Within each functional area, capabilities are evaluated against staffing, training, equipment & systems, planning & preparedness, evaluation & corrective actions, and against organization & leadership. Each rating is determined as the percentages of “current” response capabilities against “desired” response capabilities. “Current” response capabilities refer to the agency’s present ability to respond to a WMD incident, while the “desired” response capabilities refer to the current best practices, or industry standards in response capability per local, state or federal standards or guidelines.

The contribution that each functional area makes towards supporting a response to a given attack type (e.g., SCE at a transit facility) is weighted based on the expected tasks and roles a functional area would perform. These weighting factors reflect the changing roles and responsibilities of each functional area for each Attack Type. The weights for each Attack Type are applied to each functional area and sum to 1.0 so that an overall weighted average can be calculated. The overall weighted average for each Attack Type represents the jurisdiction’s preparedness for that specific attack. Figure 10 displays the results of the response assessment rating and the functional area weighted factors.

The Recovery Assessment reviews agency functions and capabilities, in an effort to manage recovery elements and business continuity following a terrorist attack to include: Plans & Procedures, Alternate Facilities, Operational Capacity, Communications, Vital Records & Databases, Tests, Training and Exercises. Figure 10 also displays a set of recovery results.

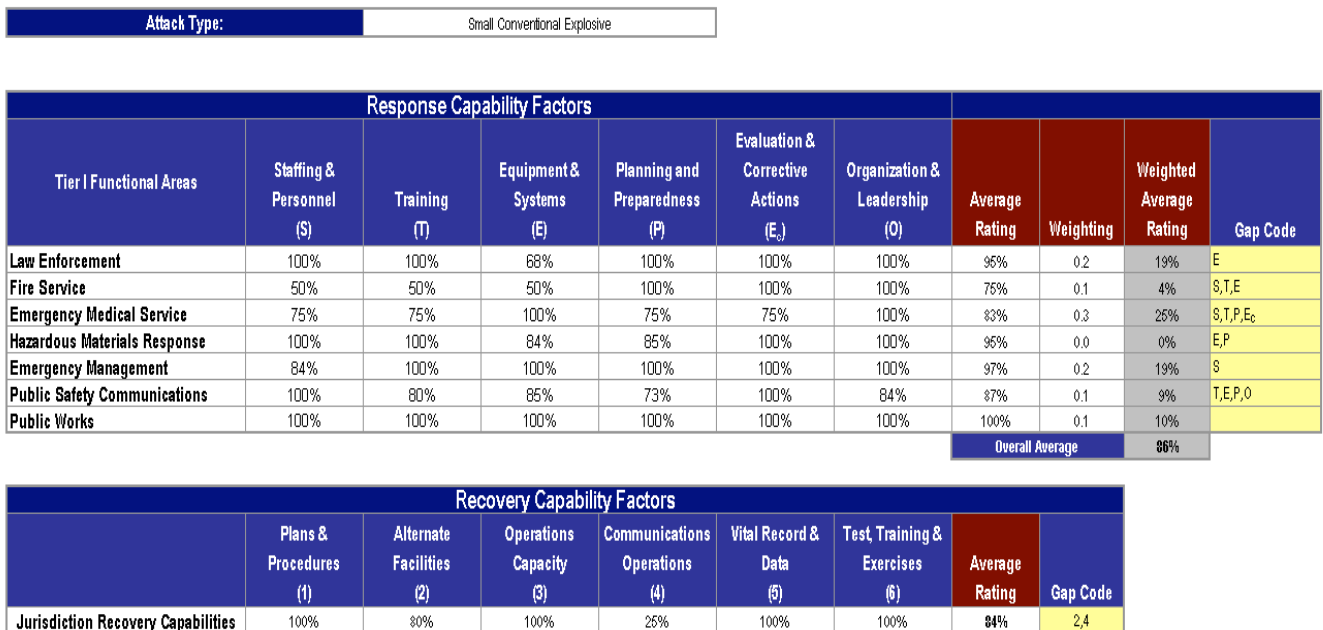


Figure 10: Example RRCA Ratings



## 7. Risk Assessment Process → Impact Assessment

The fifth component of the TRAM Risk Assessment Methodology – Impact Assessment – estimates the level of destruction to critical assets attacked using a weapon of mass destruction (WMD). Given the range of WMD types – from small explosives to biological weapons – a successful attack might not result in the total destruction of a critical asset. In addition, the capability within an organization to respond to and recover from an attack will affect overall impact. The Impact Assessment calculates the damage to a critical asset from a specific attack scenario and includes the mitigation effect of response and recovery.

The Criticality ratings for each asset form the basis for calculating Impact ratings for each attack scenario (see Figure 11). While the Criticality rating represents the asset's total contribution to the organization's mission, the Impact rating represents that portion of the asset's criticality that is lost as a result of the attack scenario given the particular attack type and delivery method. This rating is based on a scale of 0.0 - 1.0, with 0.0 representing no impact and 1.0 representing the complete destruction of the asset. It is important to note this rating is made relative to the level of criticality previously determined, not to a set value. Therefore, impact values alone are not comparable across assets. The ratings calculated in the Impact Assessment represent how effective each scenario is in evaluating an asset's contribution to the CAF. For example, assume the target is a transit station with peak occupancy of 100 employees. If an attack scenario predicts 30 fatalities or serious casualties, then the Impact rating for CAF, "Potential Casualties," is 30 out of a possible 100, or 0.3.



Figure 11: Consequence calculations.

As with the vulnerability ratings, the TRAM tool contains guideline impact ratings. These ratings are produced automatically by the tool for given scenario and asset types. The guidelines help ensure consistency across scenarios and assessments. As with all guideline ratings, the impact ratings produced by the tool are checked by experts to ensure that they are applicable to the specific asset under consideration.

Impact ratings are used, in conjunction with response and recovery ratings, to determine a Consequence rating for each CAF. The Consequence rating represents the actual level of loss for that CAF in that particular scenario. Consequence ratings are comparable between assets. For each scenario, an overall Consequence rating is calculated by summing the Consequence for each CAF. This overall Consequence rating indicates the full result of the attack scenario.

## 8. Risk Results

After the five assessments (Criticality, Threat, Vulnerability, Response Capabilities, and Impact) in the TRAM methodology are completed a risk profile can be developed for the jurisdiction. This profile is a set of scenario risk results that are plotted on a relative risk diagram. The relative risk diagram displays a visual representation of relative risk of the different attack scenarios. Risk is composed of two primary components: Likelihood and Consequence. The Likelihood rating represents the overall likelihood that an attack scenario would occur (Threat) and be executed successfully (LSA). The Likelihood for a scenario is calculated as the product of the ratings determined in the Threat and Vulnerability components of the TRAM. The Consequence rating reflects the overall expected loss of the scenario.

To facilitate plotting and comparison of scenario results, the Likelihood and Consequence ratings are normalized. The Likelihood value is normalized on a scale of 0.0 – 1.0. Each Likelihood rating is divided by (1000), the maximum actual value of the product of the Scenario Likelihood (100) and Attack Rating (10). Consequence is normalized on a scale of 0 to 100 by dividing the Consequence value for a scenario by the greatest actual Criticality value (X), and multiplying by 100.

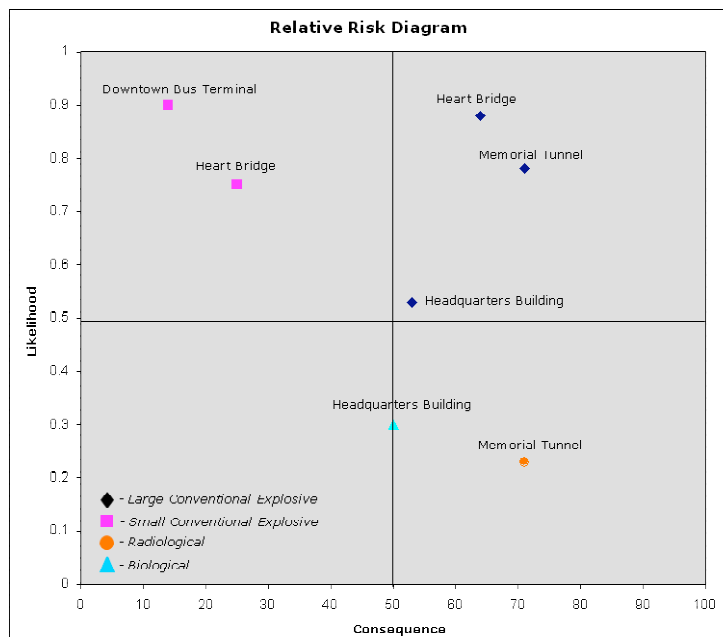
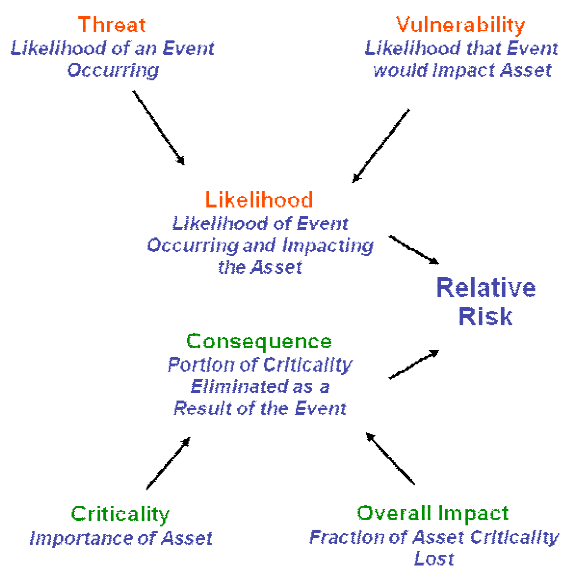


Figure 12: Overview of Relative Risk diagram

The Consequence rating, which represents the impact of a successful attack on the region, and the nation, is represented on the horizontal X-Axis and the Likelihood rating, which represents the likelihood of a successful attack occurring, is represented on the vertical Y-Axis. The relative risk diagram seen in Figure 12 shows an example of all representative scenario risk results.

The relative risk diagram is an extremely valuable tool for evaluation of the relative risk between various assets and scenarios. This diagram visually indicates which assets and scenarios carry risks that require mitigation. In addition the diagram can be used as a risk communication tool to explain the current risk faced by the jurisdiction.

## 9. Historical Risk Tracking

The second major component of the risk management process is historical risk tracking. Risk tracking is a process of looking backwards in time in order to evaluate how effective a jurisdiction has been at reducing risk and making effective investments.

The relative risk diagram serves as the heart of the risk tracking process. By comparing how the risk profile of the jurisdiction varies at different points in time, it is possible to see to what degree the risk of various events has changed. TRAM has the capability to load and compare any number of risk profiles for a jurisdiction. Figure 13 shows how changes in risk over time are displayed in TRAM. Evaluating changes in the risk of the set of scenarios over time shows how the overall risk profile of the jurisdiction has changed. Improvements in security, response, and recovery will generally result in an overall reduction of risk to the jurisdiction.

Changes in the risk profile over time can also reflect changes in the threat environment to the jurisdiction. As the threat of certain attack types changes, the position of scenarios on the risk diagram will move accordingly. Similarly, changes to the criticality of assets will also result in a change in risk and a shift of relevant scenarios on the relative risk diagram.

An important part of risk tracking is the ability to evaluate the effectiveness of particular risk mitigation projects that have been implemented between assessments. TRAM allows users to evaluate changes in risk over time to specific scenarios and to determine what changes occurred in the jurisdiction that resulted in a change in the level of risk. This allows the specific risk reduction that was achieved by the implementation of each project to be identified. Using these results, it is possible to analyze specific risk mitigation solutions that have been implemented and to compare the effectiveness of those investments.

### 10. Risk Mitigation

The final component of continuous risk management is the process of risk mitigation. Risk mitigation is the process of evaluating potential risk reduction solutions and to select those solutions for implementation that will result in the greatest possible return on investment.

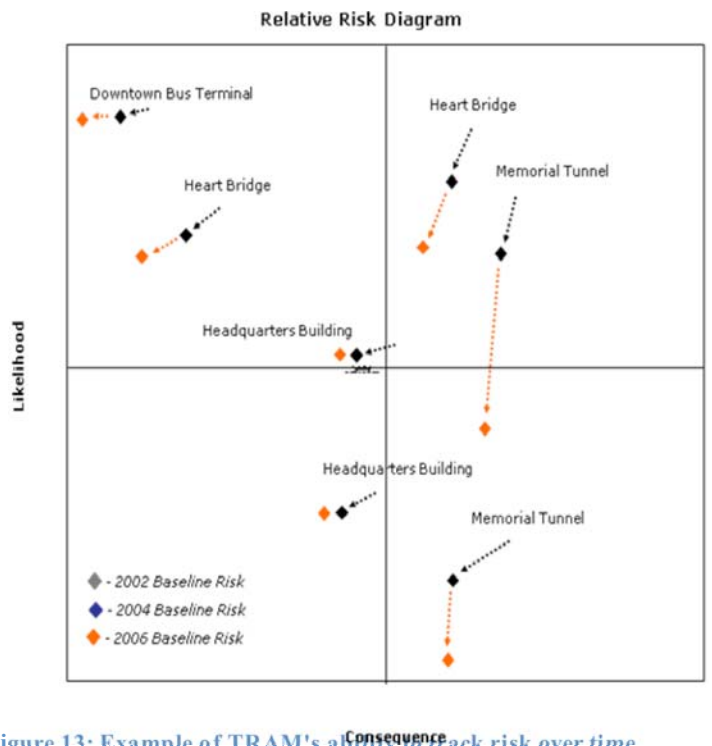


Figure 13: Example of TRAM's ability to track risk over time.

TRAM allows users to evaluate the risk reduction that would be provided by various different types of projects that might be implemented. Figure 14 demonstrates how the relative risk diagram might change based on various risk mitigation countermeasures. Improvements in security at specific assets generally improve the vulnerability ratings for scenarios at that asset. Those improvements, in turn, reduce the overall likelihood and the risk of those scenarios. Improvements response and recovery capabilities typically will reduce the impact of scenarios across the jurisdiction, reducing the consequence, and therefore the risk of those scenarios. Finally, improvements in site hardening can also reduce consequence and risk, but only for those scenarios at which the hardening is applied.

The first step in Risk Mitigation is to identify potential mitigation measures that could be implemented by the jurisdiction to reduce risk. Users identify solutions that could be applicable at each asset or across the jurisdiction. TRAM then evaluates each option alone and in combination with other options, predicting the total risk reduction that is afforded by each combination. Within TRAM each combination of options is applied to the baseline risk assessment and a new risk profile is produced, reflecting the risk profile of the jurisdiction, if that combination of projects were implemented. The difference between the new risk profile and the original baseline risk is then calculated. That difference represents the total risk reduction benefit for that set of improvements.

Potential solutions are run alone and in combination because projects are often synergistic and/or partially redundant. This reflects the concept that most effective security plans are layered in nature. Capabilities function in an integrated manner to provide protection at the asset. The evaluation within TRAM reflects these interactions and often the risk reduction provided by combination of projects will be markedly different than the sum of the projects, if applied alone.

A series of cost calculations are executed to identify the total expected lifecycle costs for the risk mitigation measures. During site visits and in subsequent internal meetings, analysts estimate the required units (i.e., linear feet of fencing or number of patrols) for each recommended countermeasure at each site. Total implementation and annual recurring costs for each are calculated based on the required units and per unit costs. The final net present cost (NPC) for each countermeasure recommendation is an initial best estimate, based on national average costs, intended to allow relative comparison between potential solutions. Actual implementation costs could vary significantly based on geography and site specific conditions, however the relative cost between projects is generally accurate. As potential projects are identified for possible implementation, cost estimates should be refined.

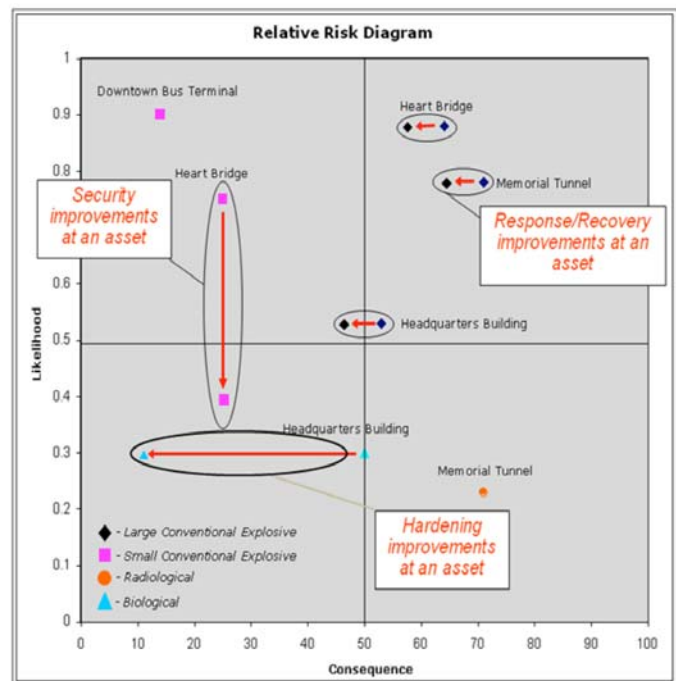
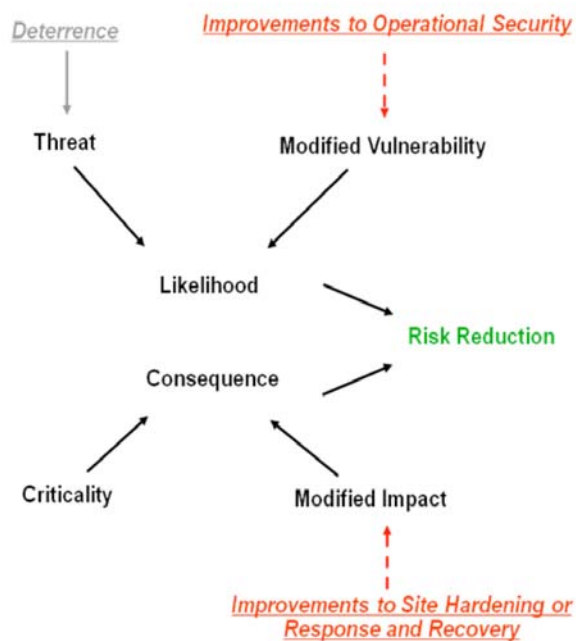
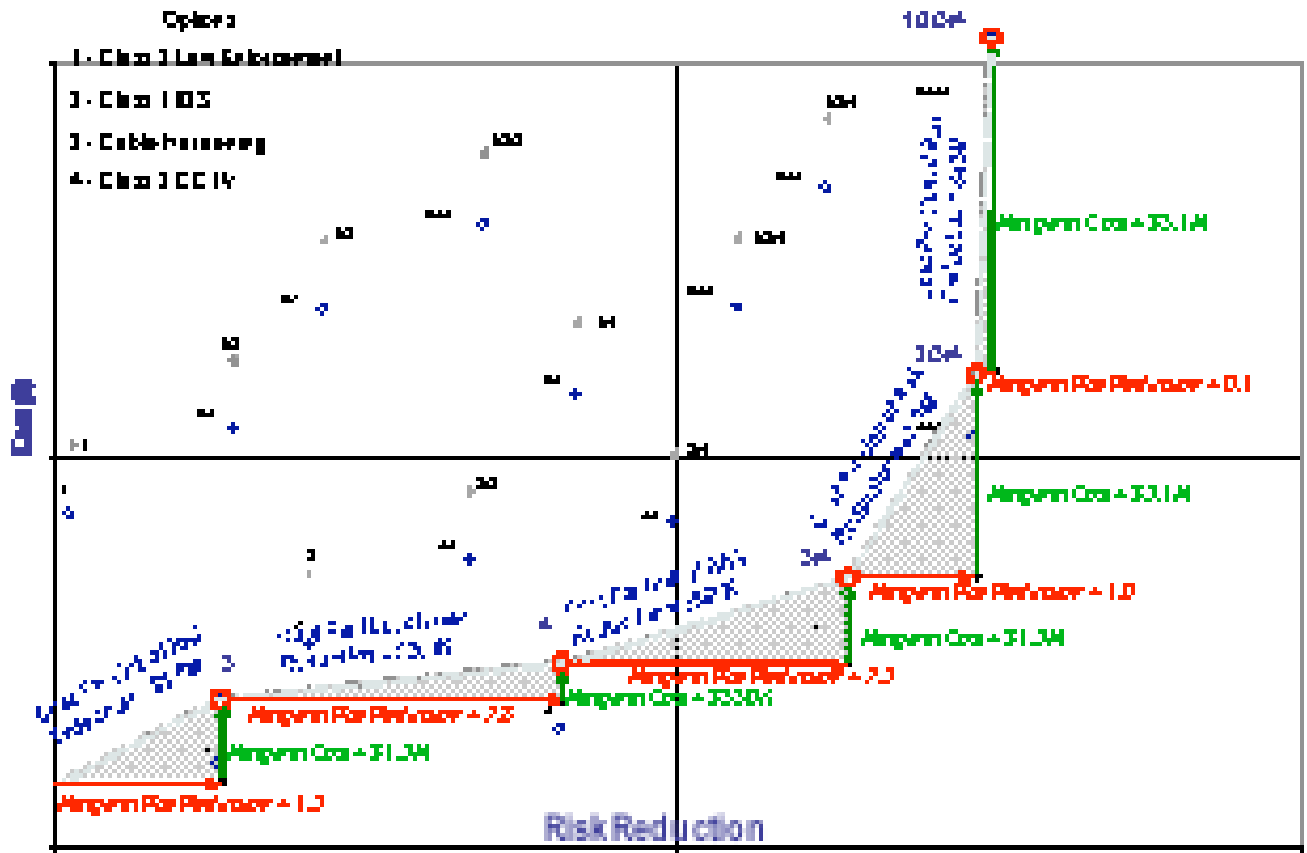


Figure 14: Risk Mitigation in TRAM



The evaluation of identified needs is conducted in the TRAM process using a Cost Benefit Analysis (CBA) technique to prioritize mitigation measures by Return on Investment (ROI). The CBA is a quantitative process which computes system-wide risk reduction benefit and lifecycle cost for various risk mitigation measures that could be employed by the organization. Based on the risk reduction and lifecycle cost for all risk reduction options, TRAM can produce CBA plots that allow for comparison of total risk reduction and cost for all recommended countermeasures and groups of countermeasures

Figure 15 illustrates a plot of CBA results for an individual asset. Each evaluated mitigation option, and possible combinations of those options, is plotted on the diagram. The risk reduction benefit of each solution is represented by the horizontal coordinate of each solution. The lifecycle cost is represented by the vertical position. Solutions that are closest to the lower right corner of the diagram offer the greatest return on investment (i.e. the greatest risk reduction for the lowest cost).

Generally, on the risk diagram, it is possible to identify a “horizon” of solutions. The horizon is defined by those solutions which provide the greatest possible level of risk reduction for any given cost. The dashed line on Figure 15 indicates those solutions that make up the horizon. Typically, the nature of the solutions that make up the horizon is that greater levels of risk reduction becoming increasingly more expensive to obtain. A certain level of risk reduction can usually be obtained relatively inexpensively. These solutions are the “low hanging fruit”. As the risk is driven out of the system, it then becomes increasingly more difficult and expensive to remove additional risk.

The marginal return on investment between each solution set can be determined by the slope of a line between the two points. The horizontal length of this line is the difference in risk reduction between the two projects. The vertical length is the difference in lifecycle cost between the two projects. The

marginal cost per unit of risk reduction for each countermeasure set therefore is calculated as the difference in lifecycle cost divided by the difference in risk. This value represents how much must be spent to purchase each additional unit of risk reduction. Countermeasure sets with the lowest cost per unit of risk reduction in a given group of options therefore represent the maximum ROI that can be achieved. Decision makers can use the cost benefit diagram to evaluate the benefits that would be available from additional investments and to select solution sets that provide reasonable returns.

It is important to note that both the calculated risk reduction and estimated costs for any countermeasure set are rough estimates. Their results should be used to identify projects as candidate for implementation. Additional analysis is usually required to better define the potential projects and to refine costs. To identify potential projects, it will be important to consider not only those countermeasure sets that form the horizon, but also those that are close to those sets on the diagram. Because of the rough nature of the cost-benefit estimates, it is entirely possible that other similar countermeasure sets could provide similar ROI.

## **11. Future Enhancements of TRAM**

The TRAM compares the relative risk of acts of terrorism against critical assets within a jurisdiction and identifies and prioritizes enhancements in security, emergency response and recovery that organizations can implement to reduce those risks. While TRAM has historically been deployed within jurisdictions to determine the risk of a terrorist attack, the Risk methodology is extendible to other (non-terrorism) hazards, including human-initiated Hazards (e.g., Theft, Sabotage, and Vandalism); Failure Hazards (e.g., Structural Failure, Equipment Failure, and Operational Failure) and Natural Hazards (e.g., Hurricane, Earthquake, and Blizzard). TRAM is currently being enhanced to permit a comparison of relative risk across all hazards – terrorist and non-terrorist and will allow for the assessment of total risk reduction benefits for proposed solutions.



Convergence of Critical Infrastructure Protection and Continuity of Operations in Banking and Finance: A Network Modeling Framework for Holistic Risk Management in the Financial Services Sector.

Steve Lieberman

**ABSTRACT**

The Federal Reserve Bank's Fedwire Funds Service (Fedwire) is a network of financial services sector participants that provides the foundation for the US economy and the backbone of the US Banking and Finance critical infrastructure sector. Banks exchange in excess of \$500 trillion per year over Fedwire, and coordinate payments with one another that both significantly increase the efficiency of the US economy while drastically reducing the intrinsic resiliency of the financial services. Recent advances in network science, along with a conceptual convergence taking place between critical infrastructure protection and business continuity strategies, have made it possible to develop and implement holistic security policies that strengthen the operational resiliency of the US economy. We highlight this convergence, with a forward-looking approach to realizing effective strategies for multiple critical sectors and reaching consensus on fundamental tools and metrics in the practice and science of critical infrastructure protection.

**AUTHOR BIOGRAPHY**

Steve Lieberman is a homeland defense and security researcher focusing on modeling and simulation approaches to critical infrastructure protection, optimizing business continuity/disaster recovery and continuity of operations management strategies in the financial services and other critical sectors, and the evolving nature of asymmetric conflict. He received a Master's degree in Homeland Security Leadership from the University of Connecticut where he developed a scientific framework for BC/DR and COOP management using network theory, organizational behavior science and statistics.

**KEYWORDS**

Critical Infrastructure Protection, Continuity of Operations, critical infrastructure policy, Banking and Finance



## INTRODUCTION

The central banking system of the United States (The Federal Reserve Bank, or FRB) is the keystone of the US banking and finance critical infrastructure sector. The Federal Reserve Bank oversees the exchange of roughly 2 trillion dollars a day between US banks and other financial sector participants. Participants send and receive money through The Federal Reserve Bank's Fedwire Funds Service (Fedwire) that allows banks to electronically transfer funds to one another throughout the business day.

Fedwire is the "Real Time Gross Settlement" (RTGS) system that provides the backbone of the US financial system<sup>1</sup>, and allows for the near immediate and legally binding transfer of money from one financial services sector participant to another<sup>2</sup>. Payment instructions are sent over an information/telecom system to the central bank which holds information about the account balances of participants. When an instruction is received, FRB debits and credits the appropriate accounts to complete a transaction. For example, if Bank A needs to pay Bank B \$100,000, Bank A will send a payment message to FRB instructing the central bank to credit Bank A's account \$100,000 and debit Bank B's account \$100,000 (Figure 1). Averages of well over 500,000 payments between roughly 5,000 different banks are processed in this way every business day<sup>3</sup>. In 2005, Fedwire processed over \$518 trillion with an average transaction value of \$3.9 million<sup>4</sup>.

One enormous benefit of processing transactions through RTGS systems like Fedwire is that banks do not have to keep large reserves of cash in their transaction accounts. Banks maintain only the amount necessary to fulfill their transactions throughout the day and keep this amount especially low by timing incoming and outgoing payments. That is, if Bank A needs to pay Bank B \$100,000, it will wait until its FRB account has been debited by the incoming payment from Bank C, which will wait for payments from other banks in the Fedwire network (Figure 2). It has been demonstrated that this timing of incoming and outgoing payments plays a major role in the US economy, allowing banks to minimize the risks associated with giving credit to other financial sector participants, and that payment coordination is severely disrupted by events affecting the critical infrastructure systems underlying the financial services<sup>5, 6</sup>.

---

<sup>1</sup> Other large RTGS systems include the Clearing House Automated Payment System (CHAPS) in the UK, the Large Value Transfer System (LVTS) in Canada, and the Trans-European Automated Real-time Gross Settlement Express Transfer System (TARGET) of the European Union.

<sup>2</sup> i.e., final and irrevocable settlement.

<sup>3</sup> Kimmo Soramäki, Morten L. Bech, Jeffery Arnold, Robert J. Glass, Walter E. Beyeler, "The Topology of Interbank Payment Flows," *Federal Reserve Bank of New York Staff Reports*, no. 243, March 2006, [http://www.newyorkfed.org/research/staff\\_reports/sr243.pdf](http://www.newyorkfed.org/research/staff_reports/sr243.pdf), accessed 10 March 2008. This report was also published as: Kimmo Soramäki, Morten L. Bech, Jeffery Arnold, Robert J. Glass, and Walter E. Beyeler, "The Topology of Interbank Payment Flows," *Physica A: Statistical Mechanics and Its Applications* 379, no. 1 (June 2007): 317-33.

<sup>4</sup> U.S. Department of Homeland Security, "Banking and Finance: Critical Infrastructure and Key Resources Sector-Specific Plan as Input to the National Infrastructure Protection Plan," May 2007, [www.dhs.gov/xlibrary/assets/nipp-ssp-banking.pdf](http://www.dhs.gov/xlibrary/assets/nipp-ssp-banking.pdf), accessed 10 March 2008.

<sup>5</sup> James McAndrews and Samira Rajan, "The Timing and Funding of Fedwire Funds Transfers," *Federal Reserve Bank of New York Policy Review*, Volume 6, Number 2, July 2000 <http://www.newyorkfed.org/research/epr/00v06n2/0007mcan.pdf>

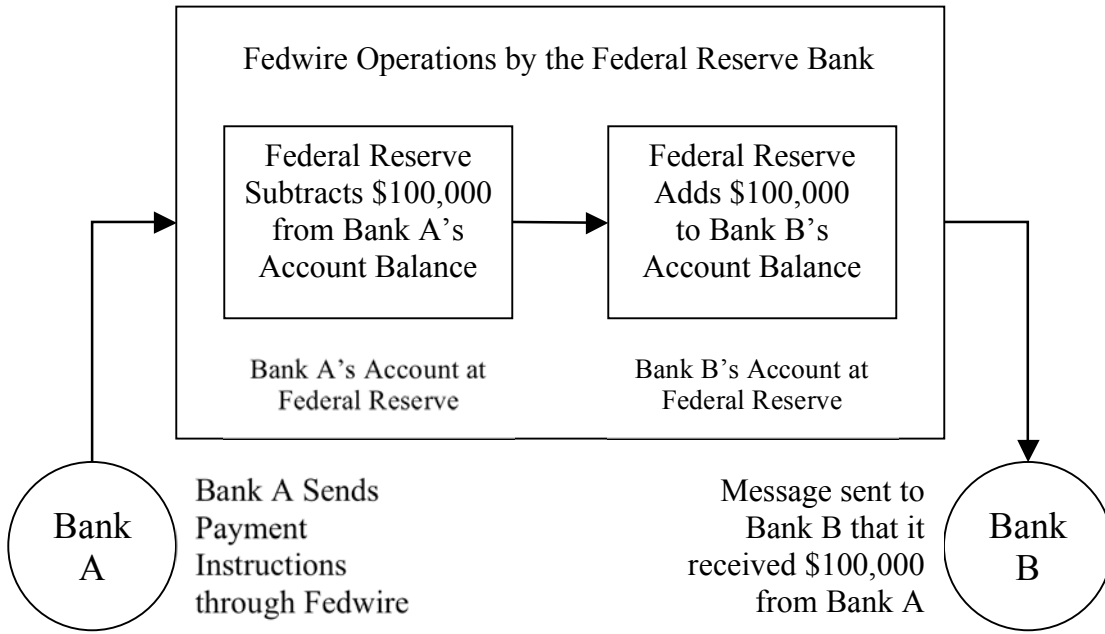


Figure 1: Transfer of \$100,000 from Bank A to Bank B using Fedwire.

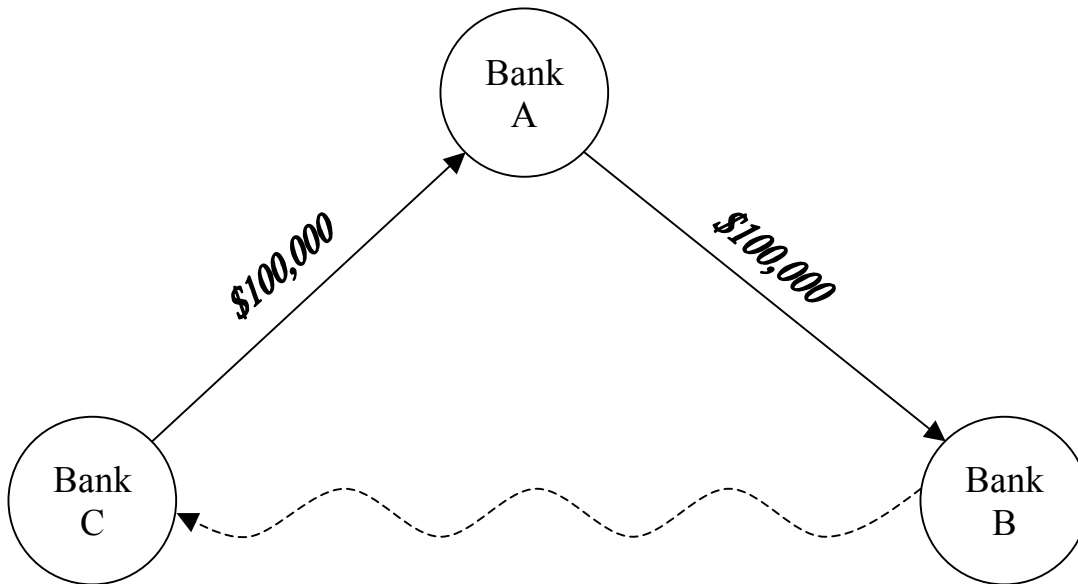


Figure 2: Bank A waits for a payment from Bank C before paying Bank B. Bank C waits for payments from other banks in the network, potentially payments from Bank B.

---

<sup>6</sup> James J. McAndrews and Simon M. Potter, "Liquidity Effects of the Events of September 11, 2001," *Federal Reserve Bank of New York Economic Policy Review*, Volume 8, No. 2, November 2002 <http://www.newyorkfed.org/research/epr/02v08n2/0211mcan.pdf> accessed 10 March 2008.

The US financial system is centered on the highly efficient clearing and settlement network provided by Fedwire. The attacks of 9/11, the Northeast blackout of 2003, and the ongoing “credit crisis” all demonstrate the continuing fragility of this vital process. Following 9/11, a great deal of effort was put in to establishing a sound basis for Critical Infrastructure Protection (CIP) in the Financial Services Sector (FSS). Over 7 years after 9/11/2001 and 6 years after requirements set forth in the National Infrastructure Protection Plan (NIPP), a comprehensive CIP framework for FFS has yet to be implemented. There are still no collectively accepted tools or metrics for achieving the level of protection and security required for Fedwire.

Here we begin to address this gap by tapping in to two areas of literature within the security profession: network analytic methods of CIP, and business continuity management strategies. Over the past several years, there is growing consensus among financial economists and security practitioners about the goals of both areas— provide continuity of operations during and after a disaster— but there has been little consensus regarding the strategies and tactics needed to reach these goals. A convergent CIP framework, such as the one outlined below, can provide CIP practitioners working in FSS with universally accepted standards to identify and address the risks posed to the networks that support the operations of critical infrastructure sectors, including Fedwire.

The Fedwire network provides the underpinnings of the US Banking and Finance sector, just as other networks provide the basis for other critical infrastructure/key resource (CI/KR) sectors<sup>7</sup>. Well-known examples of CI network models include the Power/Energy sector, which models the flow of electricity to and from residential, commercial and industrial areas, the Water sector, which models the distribution and processing of water resources, and the Transportation sector, which models the flow of people and products from one place to another. While a good deal is known about the topology and network structure of these other CI/KR sectors, relatively few investigations have been made regarding Fedwire’s topology until recently.

We will examine the Fedwire network, paying close attention to its familiar elements, its response to the terrorist attacks on 9/11/2001, and its similarity to other critical infrastructures. We address the central question of reaching consensus regarding the fundamentals of risk assessment in critical infrastructure protection, and develop the idea of conceptual convergence between business continuity management (BCM) and CIP, aimed at addressing the operational robustness of US critical infrastructure. We then outline a strategic framework based on this convergence, and apply this framework to protecting the Fedwire network.

## TOPOLOGY OF THE FEDWIRE NETWORK

We model Fedwire as a network consisting of two types of elements, *nodes* and *links*, where nodes represent financial services sector participants, and links represent the transactions between these participants over the course of a single day (Figure 3). The full collection of nodes and links-depicting an entire day’s worth of activity across Fedwire- is the network’s *topology* (Figure 4). The topology of the Fedwire network shares many of the features seen in other networked critical infrastructure models. These

---

<sup>7</sup> Ted G. Lewis, *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation* (Hoboken, New Jersey: John Wiley & Sons, 2006)

features provide insight in to the best ways to protect critical infrastructure from both natural and man-made threats, and help CIP practitioners devise strategies for optimal resource allocations across and between CI/KR sectors. One of the most instructive of these features is the presence of ‘hubs’ in the Fedwire network. These are nodes that have a great many more links than most of nodes in the network. Every day, these ‘hub’ banks send thousands of outgoing messages and receive thousands of incoming messages. The vast majority of banks in the Fedwire network send and receive considerably fewer, with almost half sending fewer than five messages per day<sup>8</sup>. Network hubs are also present in other CI/KR sectors, such as power and energy, water distribution, information and telecom and transportation<sup>9</sup>.



Figure 3: Node and link depiction of money transfer over Fedwire. There was a transaction between Bank A and Bank B during the day.

In addition to the presence of hubs in Fedwire, the network also shares additional similar and well-documented topological features with other critical infrastructure networks in terms of its connectivity. Fedwire, like networks in the water, power and telecom sectors, is simultaneously very ‘compact’ and sparsely connected. It is compact in the sense that there exist only a few links separating any two banks in the Fedwire network. The vast majority of banks in the Fedwire network are connected to each other through only one or two other banks. The nature of this compactness can be seen in Figures 4 and 5. In fact, money sent by Bank A, for instance, could end up at *any* other bank in the Fedwire network through an average of fewer than three links (transactions)<sup>10</sup>. Despite this compactness, the Fedwire network is also extremely “sparse”. It uses very few links to achieve this high level of connectivity. If every bank in Fedwire were connected by a link, there would be over 25 million links in the network. By contrast, the actual number of daily links in Fedwire averages around 76,000, or about 0.3% of the total possible links.

This combination of compactness and sparse link topology means that it’s quite easy for money to *move around* the network using few interconnections<sup>11</sup>. The route that money takes from one bank to another is called it’s “path” in the network, and the number of banks it goes through to get from one FSS participant to another is called the *path length*. The fact that each Bank in Fedwire is very closely connected to almost every other bank means that the average path length in the Fedwire network is very small. In addition to network hubs, *short average path length* is a common feature of many CI networks that have been studied over the past few years<sup>12</sup>. Investigating these paths plays a vital role in the CIP strategies we develop for the Banking and Finance sector.

<sup>8</sup> Soramäki et al., “Topology of Interbank Payment Flows”.

<sup>9</sup> For a full review, see Lewis, “Critical Infrastructure Protection”.

<sup>10</sup> Soramäki et al., “Topology of Interbank Payment Flows”.

<sup>11</sup> In the network science literature, this is commonly referred to as “The Small World Effect”.

<sup>12</sup> For a review of complex networks, see M.E.J. Newman, “The Structure and Function of Complex Networks,” *SIAM Review*, 45 (2003): 167-256.

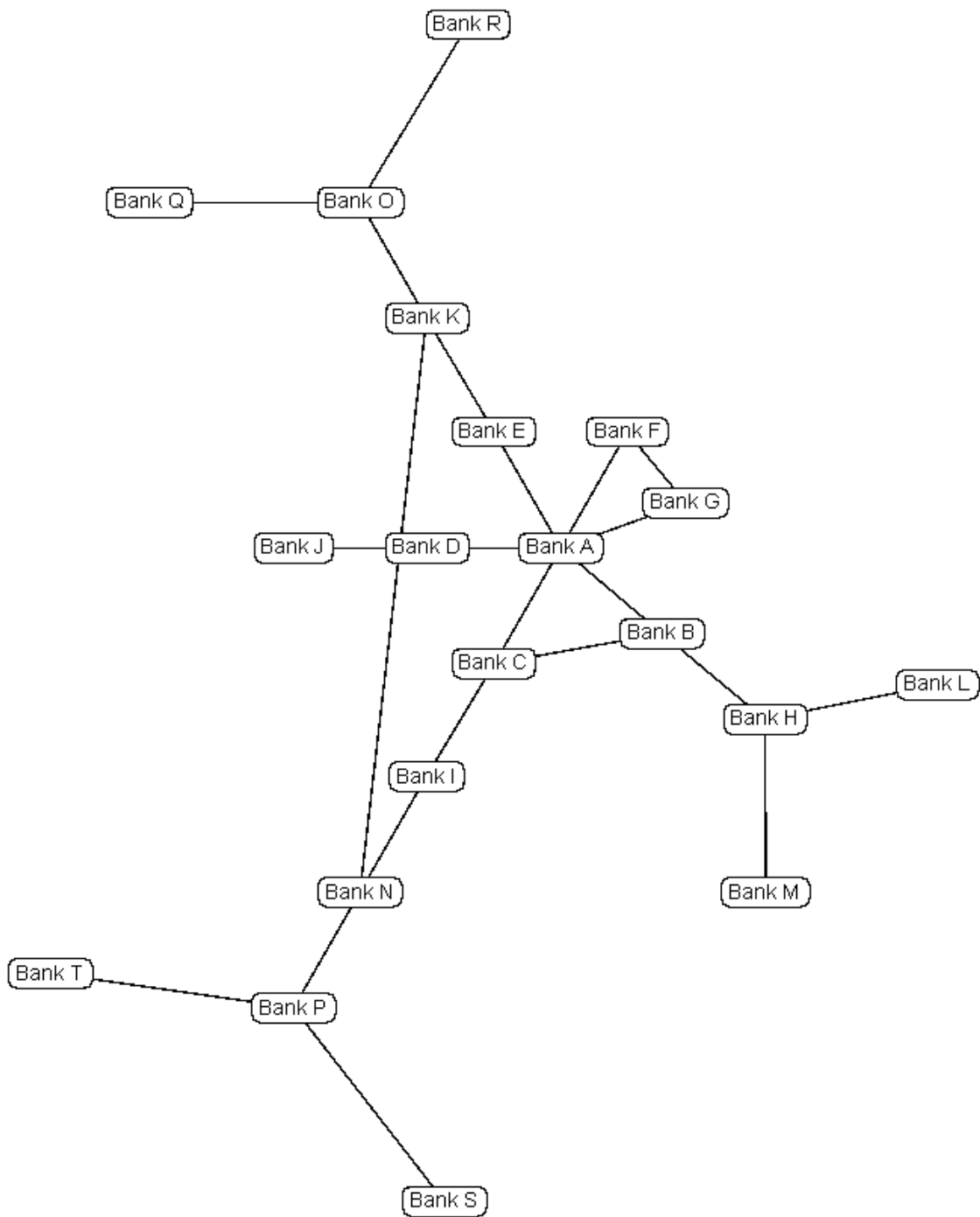


Figure 4: The full collection of nodes and links depicts a day's worth of Fedwire transactions. The above 20 banks provide a fractional representation of the approximately 500,000 daily transactions across Fedwire.

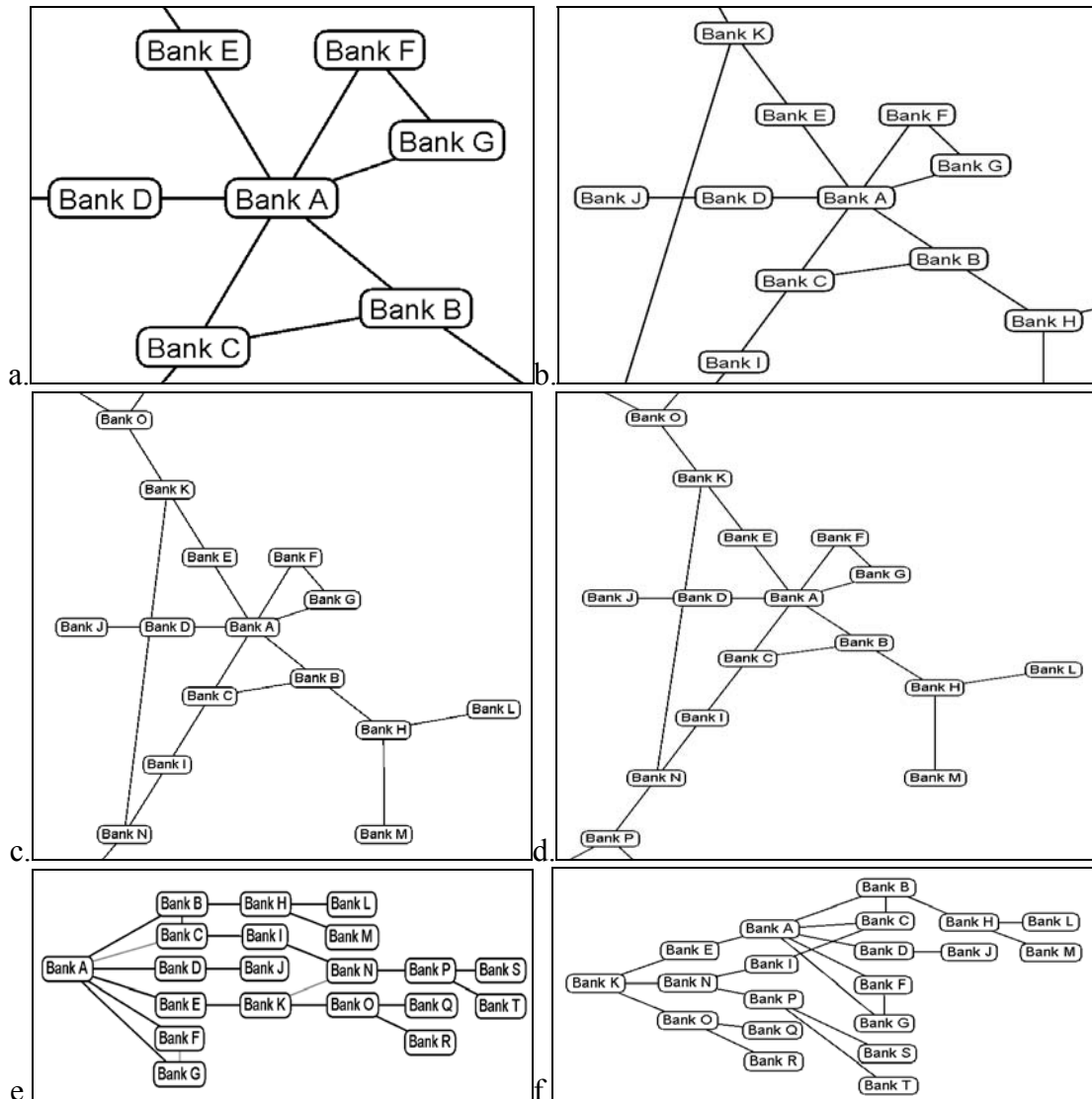


Figure 5: Cascading failures across the Fedwire network. Problem starting at Bank A, primary effects (a), secondary effects (b), tertiary effects (c), and quaternary effects (d), entire network shown in Figure 4. A Problem at Bank A would reach the entire network in just 5 steps (e), as would, for example, a problem originating at Bank K (f).

**EFFECTS OF 9/11/2001 ON THE FEDWIRE NETWORK**

The terrorist attacks of 9/11 were aimed at, among other things, destroying and disrupting the United States financial system and economic infrastructure. The attacks effected Fedwire operations in two ways. Firstly and most saliently, physical buildings and communication infrastructure was destroyed, effectively removing nodes and links from the Fedwire network—payments can no longer be received or sent—, thus the overall size of the network was reduced during the aftermath of 9/11. The destruction of physical infrastructure alone does not explain the effects of 9/11 on the US economy or Fedwire,

and CIP methods aimed at protecting physical infrastructure will likewise be ineffective at addressing the problems.

Directly following the attacks, only about 6% of the Fedwire network was removed<sup>13</sup>. More devastating to the US economy was the ripple or cascade effect that the removal of this 6% had on the Fedwire network. Since banks rely on the incoming payments of other participants to complete transactions, the 6% of banks that were effectively removed from the network had a much larger than 6% impact on the US financial services sector. The inter-bank coordination of payments that is an intrinsic part of the US economy was thrown off. Large value payments became stalled, sometimes for days. In many cases lost, destroyed or inaccessible records meant that payments could not be made at all<sup>14, 15</sup>.

Since the timing and coordination of payments is a near-universal practice among large FSS participants<sup>16</sup>, we can deduce that the initial removed of 6% of the network's nodes had an immediate effect on all of those participants' neighbor nodes (i.e., those banks that were expecting to complete transactions with a removed bank). The secondary and tertiary effects of node and link removal will continue to spread through the network until either the network is reconnected, or an outside force steps in. This is exactly what the FRB did in the wake of 9/11, providing cheap loans to FSS participants to cover the balances they expected to receive. While effective in the short term, the emergency actions of the FRB are an extremely expensive remedy to the problems caused by lapses in interconnectedness<sup>17</sup>.

## **CONVERGENCE OF CRITICAL INFRASTRUCTRE PROTECTION AND BUSINESS CONTINUITY MANAGEMENT**

“The events of September 11 underscored the fact that the financial system operates as a network of interrelated markets and participants. The ability of an individual participant to function can have wide-ranging effects beyond its immediate counterparties. Because of the interdependent nature of the U.S. financial markets, all financial firms have a role in improving the overall resilience of the financial system.”  
-Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System<sup>18</sup>

Following 9/11, there were two main security objectives within Banking and Finance: 1) to provide critical infrastructure protection for the US Banking and Finance infrastructure, and 2) to provide business continuity management for the US financial and

---

<sup>13</sup> Soramäki et al., “Topology of Interbank Payment Flows”.

<sup>14</sup> Morten L. Bech and Rod Garratt, “Illiquidity in the Interbank Payment System following Wide-Scale Disruptions”, *Federal Reserve Bank of New York Staff Reports*, no. 239, March 2006, [http://www.newyorkfed.org/research/staff\\_reports/sr239.pdf](http://www.newyorkfed.org/research/staff_reports/sr239.pdf), accessed 10 March 2008.

<sup>15</sup> U.S. Department of Homeland Security, “Banking and Finance”.

<sup>16</sup> McAndrews and Potter, “Liquidity Effects”.

<sup>17</sup> Ibid.

<sup>18</sup> Federal Reserve Bank of Dallas, “Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System.” 18 April 2003 [www.dallasfed.org/banking/notices/2003/not0321.pdf](http://www.dallasfed.org/banking/notices/2003/not0321.pdf) accessed 8 March 2008.

economic system. Business continuity management (BCM) is fundamentally concerned with the operational capabilities of whole systems. Effective BCM specifically looks at interconnectivity with the goal of keeping an organization operational at the highest possible capacity during times of crisis and change, and responding to unforeseen events with coordinated, well-planned and efficient methods.

The number one security goal of the Banking and Finance sector as outlined in its Sector-Specific Plan (SSP) is “to maintain its strong position of resilience, risk management, and redundant systems in the face of a myriad of intentional, unintentional, manmade, and natural threats”<sup>19</sup>. It then goes on to state that “the products offered by the Banking and Finance Sector are largely intangible. Thus, efforts to identify assets are largely focused on critical processes rather than physical assets”<sup>20</sup>. This coincides closely with the analyses and strategy set forth by the Federal Reserve<sup>21</sup> and other FSS publications regarding sector business continuity<sup>22</sup>.

The above analysis illustrates that the vast majority of disruptions to the US financial services sector and the US economy are caused not by the destruction of any physical infrastructure *per se*, but by the effects that this destruction has on the interconnectedness of FSS participants. One reason why it has been difficult to reach a consensus on the underlying fundamentals of risk assessment in CIP is that physical infrastructures are valued differently depending on how one interprets criticality in a CI/KR sector. Likewise, various physical infrastructures are assessed differently in terms of their vulnerabilities and the impact that their removal or reduced operational capacity would have on the CI sector following an incident.

While CIP strategies are often aimed at analyzing and protecting those elements of a sector that appear to be most valuable to its overall operation, continuity of operations (COOP) at the network level *itself* is rarely, if at all, considered. In FSS, for instance, attention will be paid as to how to best protect “important” banks, but not to protecting the underlying network that *all* banks use to support the US economy<sup>23</sup>. Just as there is consensus regarding the COOP goals of FFS, there is a general consensus that our CI elements (network nodes) are interconnected, but little attention is paid to the *interconnectedness itself*.

For instance, it is easy to think of Fedwire as a collection of banks sending payments to one another and then investigate the network to “pick out” which banks are sending the most payments, or which banks are sending the highest valued payments, and subsequently dedicate resources to protecting these banks. These traditional CIP methods are generally reductionist in design and execution—decisions are made at the level of individual components. We choose whether to protect Bank A over Bank B, and *how* to protect the bank itself. It is also “isolationist” in terms of participants, since Bank A is

---

<sup>19</sup> U.S. Department of Homeland Security, “Banking and Finance,” 2.

<sup>20</sup> *Ibid.*

<sup>21</sup> Federal Reserve Bank of Dallas, “Interagency Paper”.

<sup>22</sup> Such as, U.S. Department of The Treasury, “Improving Business Continuity in the Financial Services Sector,” December 2004 [www.treas.gov/press/releases/reports/chicagofirst\\_handbook.pdf](http://www.treas.gov/press/releases/reports/chicagofirst_handbook.pdf) accessed 9 March 2008.

<sup>23</sup> Huberto M. Ennis and H.S. Malek, “Bank Risk Failure and the Too-Big-to-Fail Policy,” (Federal Reserve Bank of Richmond) *Economic Quarterly* Volume 91/2, Spring 2005 [http://www.richmondfed.org/publications/economic\\_research/economic\\_quarterly/pdfs/spring2005/ennismalek.pdf](http://www.richmondfed.org/publications/economic_research/economic_quarterly/pdfs/spring2005/ennismalek.pdf) accessed 12 March 2008.



generally concerned with reducing its own vulnerability and not concerned with Bank B's vulnerability. In general, a business will only engage in protective measures when they enhance its individual competitiveness, and won't engage in protective measures for the purpose of enhancing the resiliency of the CI sector. Traditional methods produce a CI network that is only as strong as its weakest (or least concerned) element.

Traditional metrics and tools generally lead to both reductionist and isolationist strategies, and this is likely one major reason for the lack of a cohesive CIP framework today. Moreover, even when the effects of interconnectivity are taken in to consideration, the resulting policies often become reductionist at the level of implementation. This makes sense: it may be less intuitive to think of Fedwire as a single entity, examine CIP from that perspective, and implement policies based on this thinking. In traditional thinking, each network component is treated as an individual entity; each is treated as affecting one another, but acting alone.

It's not enough to conceptualize how *parts* affect other *parts* at the expense of ignoring the system. It is highly unlikely (arguably impossible) for the CIP community to reach consensus regarding risk analysis metrics and tools for CI/KR *sectors* (let alone a national framework) when everyone is looking at *parts*. Examining the system, holistically, enables CIP researchers and practitioners to work with the same data regarding threats and vulnerabilities, and reach the same conclusions regarding CI/KR risk analysis and protection strategies. Fortunately, there is a pre-existing body of knowledge that *does* enable us to examine continuity of operations for CI/KR sectors from a more holistic perspective: business continuity management.

## BACKGROUND

Traditional CIP focuses largely on protection of physical assets, and BCM focuses primarily on keeping processes operational. Although physical infrastructure is often necessary to perform operations, the protection of physical infrastructure should not be the *goal* of a COOP plan<sup>24</sup>. Likewise, the protection of physical buildings (banks) and communication lines (fiber optics) constituting the Fedwire network should not be the *goal* of CIP strategies for the financial services sector.

The conceptual convergence already taking place between CIP and BCM in the Banking and Finance community has produced a clear vision: the security goal must be to maintain the underlying processes within the financial services such that the *functions* of the sector are resilient to both natural and manmade incidents, and continue to operate at a very high level during major crises and wide-scale disasters. Above all, the principles of BCM involve fomenting a state of "readiness" within that aims at preventing crises, and developing an implementable response plan aimed at mitigating the effects of those crises that do occur.

The preparation- or readiness-oriented goal of a sound BCM plan is to make sure that the whole organization works together to minimize, as much as possible, the chance that something will go wrong that will require response-oriented activities. Likewise, the response-oriented goal of BCM is not to protect any one building or piece of machinery,

---

<sup>24</sup> For a thorough discussion of the variety of modern continuity goals, see for instance, The Business Continuity Institute's "Good Practice Guidelines" at <http://thebci.org/gpg.htm>, or ASIS International's "Business Continuity Guideline" at [www.asisonline.org/guidelines/guidelinesbc.pdf](http://www.asisonline.org/guidelines/guidelinesbc.pdf)

but to keep the whole organization working as best as practicable should a crisis occur. A central idea of BCM that mirrors CIP strategies of the Federal Reserve<sup>25</sup> is that responsibility for continuity of operations and maintaining a high level of system-wide capability during a crisis is spread across the organization. “Business continuity is everybody’s business”, the maxim goes.

Business continuity managers can do something that CIP practitioners working with traditional tools and metrics can not: address the *whole* system at once. BC managers recognize that an organization’s processes work interdependently, and work to make these interdependencies decisively clear. As a consequence, nearly all of the problems related to reductionism and isolationist that trouble CIP are absent. Network science fills in the pieces where traditional BCM leaves off by allowing us to conceptualize and protect CI sectors holistically. Over the last decade, developments in network science have enabled us to empirically address many long-standing questions about *how* to measure risk and vulnerability and *how* to best dedicate resources for effective BCM and CIP.

The effectiveness of network science in the development of CIP strategies has already been shown for other CI/KR sectors including power, water and telecom<sup>26</sup>. Here we assert that combining this methodology with BCM principles can lead to a comprehensive critical infrastructure protection framework for CI networks like Fedwire. As supported by the Banking and Finance SPP, and FRB publications regarding business continuity, we further assert that the majority of this effort be focused on high level *clearing and settlement* functions within the U.S. economy, and consequently protecting the operations of the Fedwire network.

## **CONVERGENCE CRITICAL INFRASTRUCTURE PROTECTION IN BANKING AND FINANCE**

“To continue to improve the resilience and availability of financial services, the Bank and Finance Sector will work through its public-private partnership to address the evolving nature of threats and the risks posed by the sector’s dependency upon other critical sectors”  
-“Vision Statement” from the Banking and Finance Sector-Specific Plan<sup>27</sup>

“The resilience of the U.S. financial system in the event of a wide-scale disruption rests on the rapid recovery and resumption of the clearing and settlement activities that support critical financial markets.”  
- Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System<sup>28</sup>

Applying a convergent framework requires that we understand the underlying processes and operations of a CI sector. Once we identify three things about the sector,

---

<sup>25</sup> Federal Reserve Bank of Dallas, “Interagency Paper”.

<sup>26</sup> Lewis, “Critical Infrastructure Protection”.

<sup>27</sup> U.S. Department of Homeland Security, “Banking and Finance,” 2

<sup>28</sup> Federal Reserve Bank of Dallas, “Interagency Paper”.

we can develop strategies and implement policy using universally accepted definitions. We must identify:

- 1) The *operational level* of the CI sector,
- 2) The *underlying network* of the operational level, and
- 3) The *risks* posed to the underlying network.

Here we provide examples of identifying the basic operational level and underlying network for three CI sectors—Power and Energy, Information/Telecom, and Banking and Finance. The crucial difference between a convergent framework and traditional CIP frameworks is that the convergent framework considers the complete sector from the very beginning. It considers *what* the sector needs to operate, *how* the sector operates in terms of a network that can be modeled and analyzed, and *why* the sector may stop functioning at full capacity. Once we identify the risks posed to the network, we can provide effective CIP for the sector.

The National Infrastructure Protection Plan (NIPP) and the Banking and Finance SSP emphasize the fact that different critical infrastructures work at different levels<sup>29, 30</sup>. The power sector, for instance, provides electricity for information and telecom. Without electricity, the information and telecom backbone of the U.S. would cease to function. This does not mean, however, that CIP strategies and policies at the information/telecom level should be developed and implemented to keep electricity flowing. Likewise, the financial services and Fedwire are dependent—in large part—on properly functioning IT. This does not mean that Banking and Finance CIP strategies should be focused on keeping IT infrastructure up and running. Rather, the *operational level* of the sector should be the focal point of CIP policy for that sector.

In much the same way that an organization can work out *contingency plans* if a supplier or large customer goes out of business, CI/KR sectors can develop contingency-like plans regarding their dependencies on other types of infrastructure. The crux of the matter is that IT cannot operate without power, and the financial services cannot operate with IT, but there are a myriad of reasons other than CI/KR sector interdependencies that a sector might fail. These other reasons are the concentration of a sector-specific CIP plan that focuses on the operational level and primary functions of the sector.

The operational level of a CI/KR sector can be determined by the commodity or resource that is distributed by the CI network. Envision CIP networks as “movers” of some commodity. The water sector moves water. The transportation sector moves vehicles, people and cargo. The power sector moves electricity. The information and telecom sector moves information. The Banking and Finance sector, then, is in the business of moving money and it is this operation—epitomized and dependent on large-scale clearing and settlement networks like Fedwire—that must be the focal point of CIP strategies at the operational level.

As an illustration of operational level and underlying network, the power and energy sector is perhaps the easiest to recognize. Its operational level moves electricity to people and places through the power grid network. It seems almost self-explanatory, but

---

<sup>29</sup> U.S. Department of Homeland Security, “National Infrastructure Protection Plan,” 2006 [http://www.dhs.gov/xlibrary/assets/NIPP\\_Plan.pdf](http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf) accessed 1 March 2008.

<sup>30</sup> U.S. Department of Homeland Security, “Banking and Finance”.

it is not without nuance. The water sector plays a major role in power and energy, too, by providing the infrastructure underpinning hydropower. Much of the US runs on the energy captured in moving water, and roughly 20% of the world's power comes from hydroelectricity<sup>31</sup>. But the Power and Energy sector is not responsible for keeping the water flowing. This is an important distinction to make when developing policy for the sector, since convergent strategies should be squarely aimed at keeping electricity flowing by addressing risks to the power grid, and developing a contingency-like plan for situations where hydroelectricity generation becomes compromised. The CIP effort focuses on risks to the underlying network itself (i.e., the power grid), since the operation of the water sector is largely outside of the control of power and energy operations<sup>32</sup>.

A convergent CIP strategy is similarly easy to apply to the Information and Telecom CI sector. The IT/Telecom sector distributes information between people and places, so its operational level involves the rapid and accurate transfer of computer data and other information (e.g., telephone calls) between appropriate parties. Even though this operation may be reliant on electricity provided by the Power/Energy CI sector, providing electricity is *not* the operational goal of the sector. The underlying network is composed of the fiber optic lines, (copper) telephone lines, relays with communication satellites, routers, switches and other network hardware that link personal computers, servers and telephone systems together.

The principles of BCM work to keep the information flowing through this CI network. A convergent CIP strategy in IT/telecom therefore has both 'readiness' and 'response' goals, and focuses on, 1) maintaining an information transfer network that intrinsically minimizes the probability that information transfer will be negatively impacted by outside events (i.e., the network itself has built-in mechanisms that prevent crises), and 2) designing an information transfer network that quickly and effectively restores accurate information transfer between appropriate parties during and after a disaster (i.e., the network itself has built-in mechanisms that respond to those crises that do occur).

A good deal of attention in the financial services sector has been given to securing the underlying IT infrastructure upon which networks like Fedwire operate<sup>33</sup>. While many questions have been raised concerning the best way to achieve this goal, there is very little agreement about what to do, or even where to begin. Since Banking and Finance works "on top of" IT infrastructure, this may seem an intuitive and easy place to start. But the operational goal of Banking and Finance is money transfer, not providing IT/Telecom.

The operational goal of Banking and Finance is to provide a medium for highly efficient and highly precise funds transfer through networks like Fedwire. The Banking and Finance sector analog to the convergent CIP strategy for IT/Telecom focuses on, 1) maintaining a funds transfer network that intrinsically minimizes the probability that

---

<sup>31</sup> Renewable Energy Policy Network for the 21<sup>st</sup> Century, "Renewables: Global Status Report, 2006 Update" [http://www.ren21.net/globalstatusreport/download/RE\\_GSR\\_2006\\_Update.pdf](http://www.ren21.net/globalstatusreport/download/RE_GSR_2006_Update.pdf) accessed 20 March 2008.

<sup>32</sup> The result is analogous to each business in a supply-chain network developing its own continuity plan, and thus effectively strengthening the resiliency of the entire supply-chain.

<sup>33</sup> United States General Accounting Office, "Critical Infrastructure Protection: Efforts of the Financial Services Sector to Address Cyber Threats," January 2003 [www.gao.gov/new.items/d03173.pdf](http://www.gao.gov/new.items/d03173.pdf) accessed 10 March 2008.

clearing and settlement activities will be negatively impacted by outside events, and 2) designing a funds transfer network that quickly and effectively restores clearing and settlement activities between appropriate parties during and after a disaster.

## PROTECTING THE FEDWIRE NETWORK

We now turn to the application of a convergent model to protection of the Fedwire network, identifying the specific risks to Fedwire, and developing strategies to reduce the likelihood that the US economy will be disrupted by natural or manmade incidents that impact the critical infrastructures underlying the financial services sector. The Interagency Paper on Sound Practices of Strengthen the Resilience of the U.S. Financial System concentrates on hardening the clearing and settlement functions supporting the U.S. economy. The Banking and Finance SSP focuses specifically on the Fedwire, the clearing and settlement network of the Federal Reserve Bank.

Financial economists, business continuity experts and critical infrastructure practitioners agree that the operation of Fedwire is fundamental to the strength and stability of the United States financial system. Current BCM literature and CIP literature in Banking and Finance converge on two other core concepts: 1) the financial services sector is essentially the entity that moves money and monetary assets through a network of rights holders (FSS participants), and 2) the sector relies on a network of interdependent processes to perform this fundamental task. These facts culminate in the reality that effective CIP in Banking and Finance must essentially be a *process*-focused enterprise.

With this in mind, the goal is relatively straightforward: design and maintain a robust underlying network for funds transfer that minimizes the potential for disaster and quickly restores activity should one occur. But the precise strategies and policies needed to reach these goals can be complex. Accordingly, formulating appropriate strategies requires a meaningful understanding of the risks posed to CI sector operations and the underlying network.

## GRIDLOCK AND DEADLOCK

Bech and Soramäki outline two major risks to the operation of clearing and settlement networks like Fedwire: *gridlock* and *deadlock*<sup>34, 35</sup>. Both of these problems arise when money cannot flow through the network as usual (Figure 5a), as was the case following the attacks of 9/11 when roughly 6% of banks in the Fedwire were removed from the network. A *gridlocked* network refers to a state where Bank A requires a payment from Bank B in order to pay Bank C. That is, Bank A does not have enough money on hand to pay Bank B without first receiving payment from Bank C (Figure 5b). In a gridlocked network Bank A is waiting on Bank B, Bank B is waiting on Bank C, and

<sup>34</sup> Morten Linnemann Bech and Kimmo Soramäki, "Liquidity, gridlocks and bank failures in large value payment systems," *Emoney* 1/29/2002: 113-127 [www.soramaki.net/papers/Bech-Soramaki\\_01\\_EMR.pdf](http://www.soramaki.net/papers/Bech-Soramaki_01_EMR.pdf) accessed March 9 2008.

<sup>35</sup> Kimmo Soramäki and Morten L. Bech, "Gridlock Resolution in Interbank Payment Systems" *Bank of Finland Working Papers*, no. 9/2001, 13 June 2001 [www.nationalbanken.dk/.../9b01ad8183f05397c1256e7b0040dc54/\\$FILE/2001\\_MON4\\_grid67.pdf](http://www.nationalbanken.dk/.../9b01ad8183f05397c1256e7b0040dc54/$FILE/2001_MON4_grid67.pdf) accessed 10 March 2008.

so on. Gridlocks can be resolved when all banks in the payment path have enough money in the account balances to settle simultaneously. That is, if the net amount owed to each FSS participant was transferred at the same time, no participant end up with an overdraft. If this is not the case, the network is *deadlocked* (Figure 5c), and an outside source (such as the Federal Reserve Bank) must provide money for transactions to resume across the network.

The coordination of payments throughout Fedwire and the low cash reserves that banks keep in their accounts enable gridlock to quickly spread throughout the clearing and settlement network. Without effective CIP policy in place, this type of cascade will rapidly affect the majority of clearing and settlement activity, destabilizing the United States financial system and economy, and requiring expensive government intervention in the form of liquidity injections by the Federal Reserve<sup>36</sup>.

Using the “preparation” and “response” criteria from business continuity management, the gridlock and deadlock risks identified by economists and financial policy experts, and contemporary critical infrastructure protection theory, effective CIP in the Banking and Finance sector means, 1) preparation to prevent gridlocks and deadlocks whenever possible, and 2) the ability to quickly and effectively respond to any gridlocks or deadlocks that occur.

Implementation of the convergent framework requires that we model the CI sector as a network of nodes and links that moves a commodity, in this case money, from place to place. Since gridlocks and deadlocks can be modeled as events taking place on the Fedwire network, developments in network theory can guide our strategy. Working with network models also allows us to identify risks and vulnerabilities at the network level (i.e., for the entire CI/KR sector), and simulate the effects of our strategies during failure conditions on the network. In particular, the identification of network hubs and critical paths allows us to both prepare for and respond to gridlocks in terms of the *system* instead of individual components.

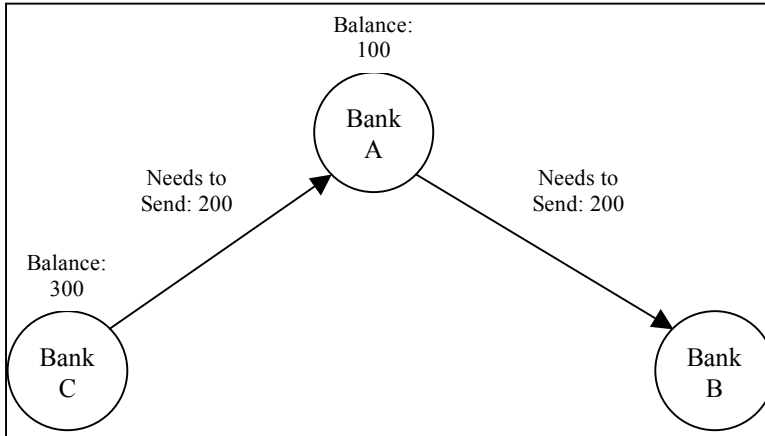
## IDENTIFYING FEDWIRE HUBS

As mentioned above, there are a great many similarities between well-studied CI networks, such as water and power, and Fedwire, such as the presence of network hubs and short average path lengths. Consequently, we can look to the strategy and policy pertinent to other CI sectors for some guidance. There are, however, important differences between Fedwire and other CI networks. One important difference is that, unlike CI networks for water and power, the hubs in Fedwire can and do change daily.

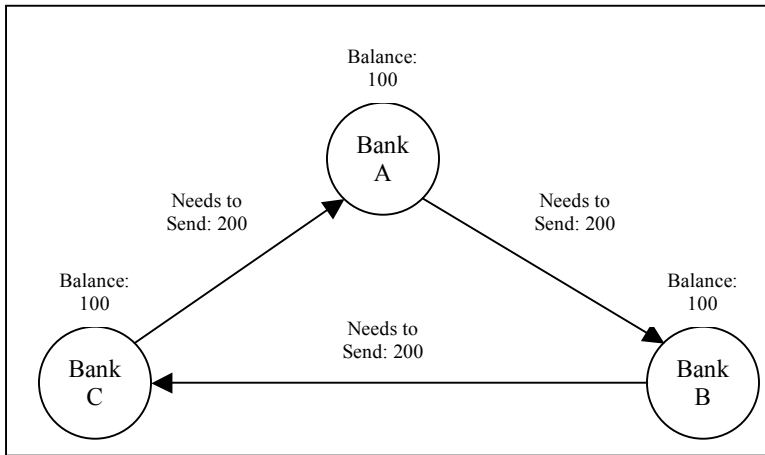
To formulate effective CIP strategies for the Fedwire network, we can first identify the network’s hubs. This is more complex for Fedwire than some other CI networks. While at the time of this writing there is no universally agreed upon method for distinguishing the probability that a single bank will be critical to the network from day to day, we can add to the literature by substantially narrowing down the potential candidates. We do this by coupling financial modeling with insights garnered from network science and other CI sectors.

---

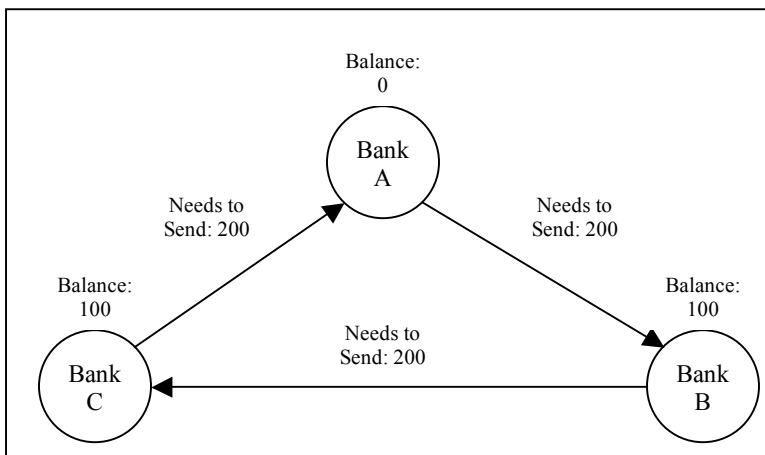
<sup>36</sup> These effects were seen following 9/11 and, more recently, at many point during the ongoing “credit crisis” that has depressed the world economy and led to the bankruptcy of numerous small and large banks.



a. Regular Payment Coordination: Bank A has an account balance of 100 and waits for a 200 payment from Bank C before sending 200 to Bank B. In this case, the account balance of Bank C is inconsequential.



b. A Gridlocked Network: Each bank needs to send 200 but only has an account balance of 100. This cluster can be solved by transferring all money simultaneously (i.e., netting).



c. A Deadlocked Network: Each bank needs to send 200 but the account balance of Bank A is 0. This cluster cannot be solved by netting alone. Bank A must receive 100, then the cluster can be solved by netting as above.

Figure 5: Payment Coordination and Risks to Fedwire Operation. Regular payment coordination (a), gridlock (b), and deadlock (c).

The number of transactions a bank engages in can vary widely from day to day, but there are a limited number of FSS participants that are likely to be hubs. In their study of Fedwire topology, Soramäki *et al.* found a *core component*<sup>37</sup> of Fedwire that consists of the *same* 2,578 banks every day<sup>38</sup>. This represents roughly 37% of the complete network. We can further reduce the number of banks that are likely to be hubs in three ways. First, we know that the daily hubs have about 2,000 outgoing links while 50% of banks in the Fedwire network have fewer than 5 outgoing links. Secondly, we know that when banks participate in many transactions they tend to link to banks with only a few connections, instead of hubs<sup>39</sup> (Figure 6). Lastly, we can look at the historical data regarding number of transactions for each bank in the core, keeping in mind the effects of periodicity—for instance, a bank that makes a large number of transactions on one day may be more or less likely to make a large number of transactions the next day.

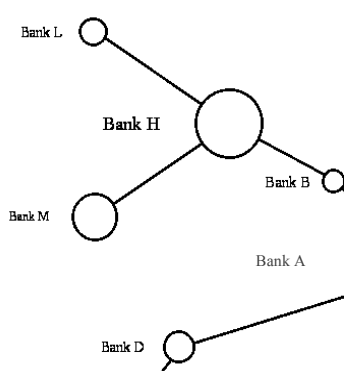


Figure 6: Depiction of partial model Fedwire network showing relative sizes of banks. Larger size is equivalent to a greater number of transactions in Fedwire.

Taken together, these statistics allow us to calculate the probability that any single bank will be critical on any given day. With the right information, we can limit the number of potential hubs to a handful of banks. This enables us to concentrate on those banks in much the same way that we concentrate on hubs in other CIP networks, paying close attention to conditions that

might put the Fedwire network at increased risk.

Identifying network hubs, however, is not enough for a sound CIP strategy. The reason a ‘protect the hubs’ strategy works for CI/KR networks, in general, is the same reason it is necessary but insufficient to constitute a comprehensive strategy for Banking and Finance. Hubs must be protected, the reasoning goes, because the greatest number of resources (water, electricity, information) will move through them. Hubs will channel the commodity throughout the network and without hubs, the network operation will be either severely restricted or cease altogether. The commodity in question, however, still needs to arrive at a hub in the first place, and continue along its path to where it is needed.

This problem is particularly germane to the FSS where the coordination of payments plays a major role in the clearing and settlement process. Even the hub banks in the Fedwire network rely on incoming payments to complete transactions. Banks of all sizes coordinate their payments with one another throughout the day to keep their cash reserves as low as possible and minimize their exposure to certain types of risk (e.g., settlement risk<sup>40</sup>). What’s more, banks will generally attempt to time *all* of their payments in this way. Thus, if Bank A—a hub in the Fedwire network—send 2,000

<sup>37</sup> In network theory literature this core component is generally referred to as the “Giant Strongly Connected Component”.

<sup>38</sup> Soramäki *et al.*, “Topology of Interbank Payment Flows”.

<sup>39</sup> This is called disassortivity or dissortivity in most network science literature.

<sup>40</sup> Settlement risk refers to the risk that an incoming payment will not come through as planned.



payments out, we can expect that Bank A will receive approximately the same number<sup>41</sup>. We must be able to identify the path that money needs to take within Fedwire. For instance, the images in Figure 5 depict the path of 200 from Bank A to Bank B to Bank C.

## IDENTIFYING CRITICAL PATHS

Another CIP insight that we can glean from investigating network topology is what paths are most critical to the functioning of the sector. By analogy, consider the water sector. If there is a hub in the water sector that is responsible for pumping and distributing clean water to millions of Americans, then it makes sense to protect that hub, especially if there is no readily available backup. If that critical element in the water infrastructure is fed primarily by a large reservoir then we must consider that reservoir a critical element as well, even if it has only a single connection in the network—it's link to the pumping and distribution facility.

Network hubs will be part of critical paths, in general, regardless of the network or CI/KR sector<sup>42</sup>. Correspondingly, a convergent CIP strategy must also consider the ways in which we can best allocate resources to hardening and protecting *critical paths* in networks, and this is illustrated below with regards to Fedwire. Fortunately, the history and practice of BCM offers numerous methodologies as well as examples (both successful and unsuccessful) of critical path protection<sup>43</sup>.

Since incoming payments are used to make outgoing payments across the network throughout the day, simply protecting the hubs of the Fedwire network will not protect the clearing and settlement process. Protecting hubs will not stop gridlock or deadlock. If the Fedwire network becomes gridlocked, outgoing payments become queued as banks wait for incoming payments. The longer the gridlock exists, the larger the queues become.

If a hub bank starts building a queue, it could be detrimental to Fedwire operation. Since the hub banks generally make about 2,000 payments per day, a large percentage of the Fedwire network will be immediately affected by any delay. Given the connectivity of Fedwire, it is likely that the secondary effects—i.e., simultaneous queues at the 2,000 recipient banks— would affect almost all of the Fedwire network and US financial system<sup>44</sup>.

Critical paths are those that affect a large part of the network, and it's clear that hubs are generally part of critical paths. However, due to the fact that hub banks tend to link to banks with only a few connections, most critical paths in the Fedwire network will involve one hub and many banks with few links. A probable scenario leading to widespread gridlock involves a large hub bank waiting on a high-value payment from a smaller bank (Figure 7).

---

<sup>41</sup> This is supported both in theory (e.g., McAndrews and Potter, "Liquidity Effects") and by empirical studies of network transactions (e.g., Soramäki et al., "Topology of Interbank Payment Flows").

<sup>42</sup> Of course, this is only true in networks that have hubs. Some networks have a more homogenous distribution of links. Thus, even though there might be critical paths, there are no network hubs.

<sup>43</sup> See Kenneth Myers, *Business Continuity Strategies: Protecting Against Unplanned Disasters* (Hoboken, New Jersey: John Wiley & Sons, Inc., 2006)

<sup>44</sup> In these situations, banks borrow money from major lending sources such as The Federal Reserve Bank.

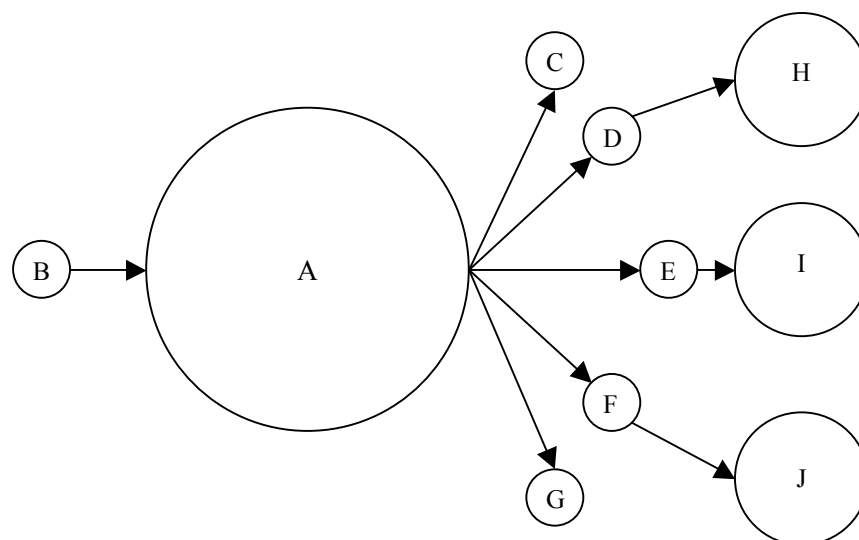


Figure 7: Critical paths through large and small banks. Larger size is equivalent to greater number of transactions in Fedwire. Both the small Bank B and the large Bank A are critical to the rest of the network. A problem originating at small Bank B can shut down Fedwire operations. (Arrowheads indicate direction of money flow.)

## STRATEGY DEVELOPMENT

Developing a convergent CIP strategy for Banking and Finance requires that we address *both* gridlock and deadlock in the Fedwire network. The “gridlock resolution” methods currently proposed in the literature are algorithms that will inspect payment queues and identify the largest collection of pending payments that can be settled simultaneously without resulting in an overdraft<sup>45</sup>. The gridlock resolution algorithm is effectively an on-demand netting system since each bank affected by the algorithm’s implementation will end up with the ending (net) amount as if all of the transactions taking place one at a time. In Figure 5, for instance, all banks transfer 200 and end up with balances of 100. But gridlock resolution mechanisms cannot address Fedwire deadlocks.

Deadlocks cannot be solved by netting when at least one bank in a payment path would end up with an overdraft. To resolve deadlocks, banks must borrow money and a major source of this funding is the Federal Reserve Bank, which has historically lent money to banks at favorable rates during times of crisis. Like most current practices, such lending is reductionist and isolationist in the sense that banks are each considered individually and a loan is made if deemed appropriate.

Enough lending through can theoretically resolve any deadlock, but it comes at an enormous price. Such lending increases the delays associated with payment coordination across the Fedwire network, costs the US economy in interest payments, and exposes the Federal Reserve System to large amounts of credit risk. The FRB is understandably

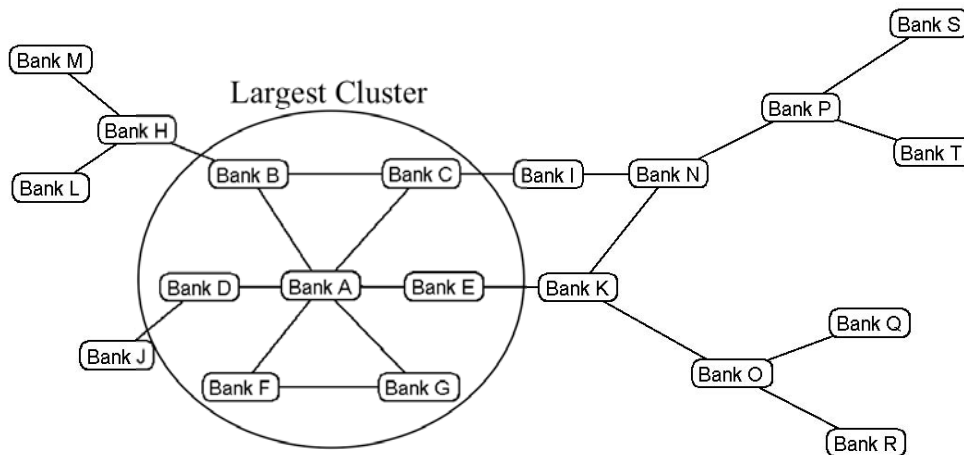
<sup>45</sup> See Bech and Soramäki, “Gridlock Resolution”. For a brief review of settlement simulations see, Donatas Bakšys and Leonidas Sakalauskas, “The System for Simulating Interbank Settlements,” *Technological and Economic Development of Economy*, Volume XIII, no. 4 (2007): 323-332 [www.tede.vgtu.lt/upload/ukis\\_zurn/2007\\_4\\_baksys.pdf](http://www.tede.vgtu.lt/upload/ukis_zurn/2007_4_baksys.pdf) accessed 12 March 2008.

cautious about loaning more money than is needed, and the recovery time from a wide-scale disruption is inherently extended by these considerations. Problems are further exacerbated by the fact that gridlocks and deadlocks are treated separately when they could be treated simultaneously by a comprehensive CIP plan the focuses on continuity of operations in the financial services.

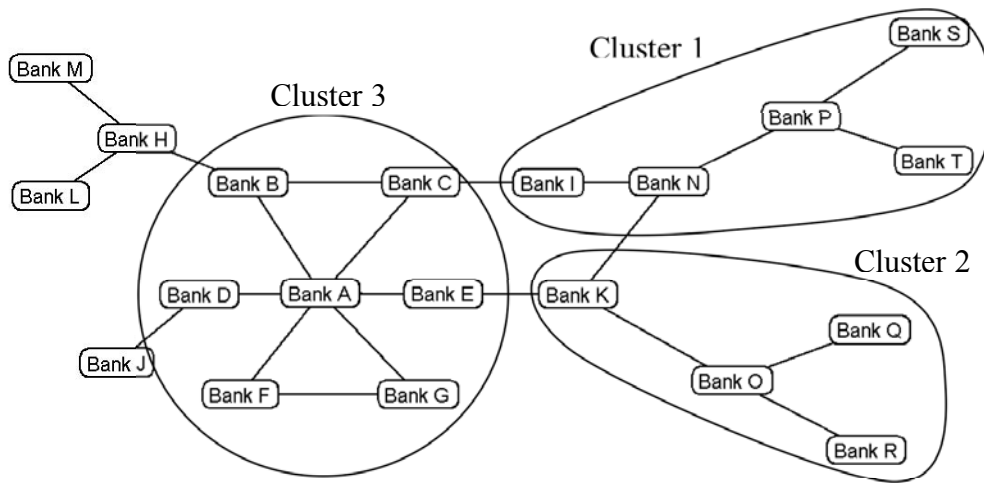
The real-time and ongoing identification of network hubs and critical paths can allow the Fedwire network to “heal” itself in a way that permits the clearing and settlement of all gridlocked and deadlocked payments in the system. Modern networked computer systems could make this process transparent, seamless and near-instantaneous. Using the tools of network theory, we can identify clusters of payment queues that can be settled using gridlock resolution methods. Unlike the existing methods, however, the algorithm would not look for the largest set of payments to settle simultaneously. It would, rather, look for and settle those clusters of payments that would permit the whole network to resume normal operation as quickly as possible.

Because of the differences in account balances before and after settlement, and the process of payment coordination, a *path-based* gridlock resolution method allows for a greater number of settlements to take place between a larger set of banks in a shorter period of time. “Solving” one cluster after another means a greater number of payments will be completed in a shorter period of time than attempting to solve the largest set of payments at once (Figure 8). Addressing payment clusters sequentially can fix system-wide problems more efficiently than the current gridlock resolution algorithms.

Path-based gridlock resolution (PBGR) addresses half of the problem. When the network is deadlocked, there must be a mechanism for providing the appropriate amount of quick liquidity to those banks that need it in order for Fedwire to return to normal operations. PBGR can be combined with an efficient liquidity system that would lead to the *most* gridlock resolution and require the *least* amount of liquidity injection to resolve network deadlock. This system can be highly efficient loaning only the minimum amount of money needed to enable PBGR by injecting liquidity at specific sites in the Fedwire network. The combination of Path-Based Gridlock Resolution (PBGR) and the Automatic Local Liquidity Injection for Efficient Settlement (ALLIES) meets all of the CIP goals for the Financial Services Sector. For simplicity, we will call the combination of PBGR and ALLIES *Automated Cascading Cluster Settlement*, or ACCS.

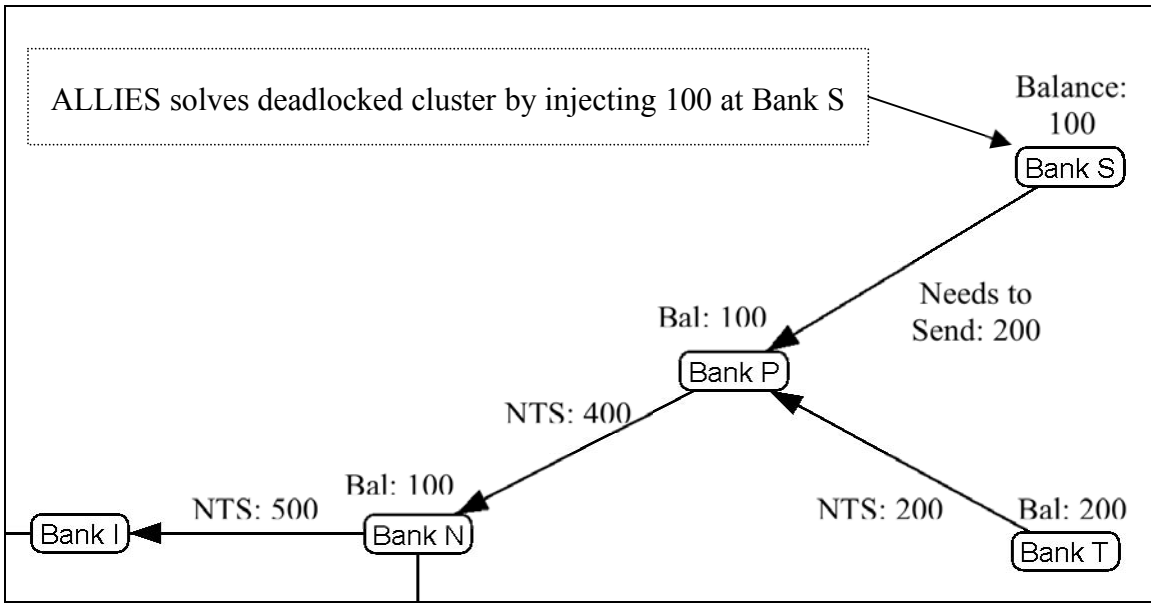


a. Largest cluster in a gridlocked network. Existing gridlock resolution methods solve for the largest cluster of banks in a gridlocked network at any one time. The existing methods might solve a central cluster of banks, but ignore other banks within Fedwire’s critical paths (such as Bank S, or Bank O), leading to more government intervention (liquidity injection) and extending the duration of a financial crisis.

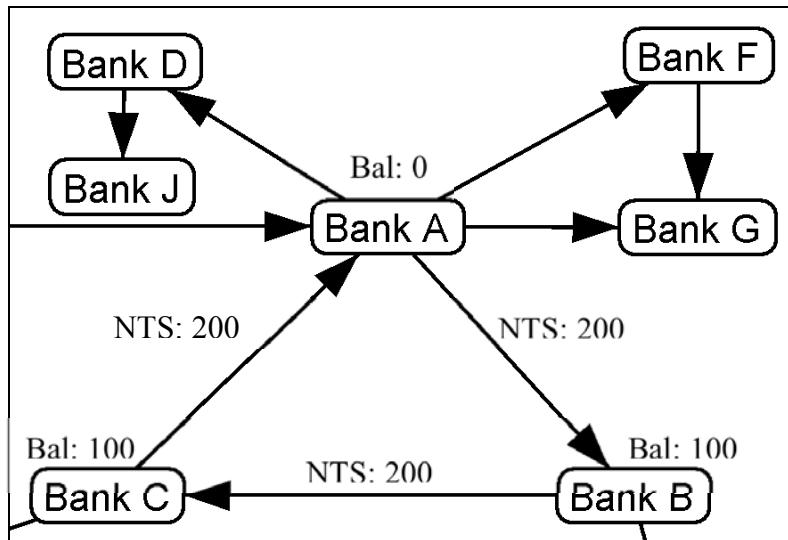


b. Settlement of three clusters along a critical path. Path-Based Gridlock Resolution (PBGR) solves clusters of banks in the order that allows for the greatest number of accounts to be settled across the entire Fedwire network. Suppose a critical path exists from Bank N → Bank K → Bank E → Bank A. PBGR starts by investigating the upstream dependencies from network hub Bank A, dividing the network in to three clusters that can be settled one after the other for the most efficient resumption of Fedwire trading activity. Settlement of cluster 1 permits Bank N to send payment to Bank K, which allows the settlement of cluster 2. Resolution of gridlock in both cluster 1 and cluster 2 allows cluster 3 to be settled, which permits settlement of the entire network.

Figure 8: Depictions of existing gridlock resolution methods (a), and Path-Based Gridlock Resolution (b).



a. Detail of cluster 1 from Figure 8b. ALLIES resolves deadlock in cluster 1 by injecting 100 at Bank S, allowing the cluster to be solved by PBGR.



b. Detail of deadlock from Figure 5c. ALLIES can resolve this deadlock by injecting 100 at Bank A, then the cluster can be solved by transferring all money simultaneously between Banks A, B and C (i.e., netting). Traditional systems result in a loan of 200 to Bank A, double the amount necessary to settle payments using ACCS.

Figure 9: Operation of Automatic Local Liquidity Injection for Efficient Settlement (ALLIES) for solving deadlocks in a cluster (a) and between three banks (b).

An intelligent system with information about all payment queues and account balances in the Fedwire network will be able to identify where the least amount of money is needed to resolve local deadlocks between banks. An ACCS system can be designed to first look at those banks that are most likely to be Fedwire hubs since these hubs are most likely to lie along the critical paths in Fedwire. Investigating the upstream and downstream (i.e., incoming and outgoing) paths from hubs will be the quickest way to ascertain *precisely* why money is not flowing through the system as usual, and correct the problems.

Analyzing these potential critical paths in parallel can quickly elucidate how to settle accounts without excess liquidity injection. Our criterion can be total number of payments, total value of payments, or some combination, so long as the ACCS system has access to information about all pending payments in Fedwire. The system can investigate payment clusters within Fedwire, settle clusters of several banks at a time that do not require any liquidity injection, and result in the transfer of money to a bank that would have otherwise required a loan. Thus, in a large number of cases we may be able to *avoid* deadlock altogether, even during financial disasters such as the credit crisis and the aftermath of 9/11.

A detailed explanation of ACCS system operation and its implementation is beyond the scope of this paper. Further research is needed to determine how a system would be deployed, and the precise implementation and deployment of an ACCS system will be a matter of policy development (as described in the next section). Nevertheless, the technological foundations for ACCS are in place as of this writing. Recent publications have paved the way for major developments in the design of “self-healing networks” (SHNs)<sup>46,47</sup>, and there exist several candidate systems on top of which ACCS could be built, including the Secure Financial Transaction Protocol (SFTP) and the Resilient Financial Transaction System (RFTS) design<sup>48</sup>. As outlined in the Banking and Finance SSP, research and development activities regarding these systems is an ongoing priority, with the number one R&D priority being the development and deployment of “protection and prevention systems” in the Banking and Finance sector<sup>49</sup>.

## POLICY IMPLIMENTATION

Now that we have outlined the foundations of a strategy to reach our CIP goals, we consider the fundamentals of implementing a policy based on our strategy of addressing CIP at the operational level. Namely, we must outline an actionable policy for

---

<sup>46</sup> See Abdullah Gani and G. Manson, “Towards a Self-Healing Network in Controlling Access to Network Applications,” *Informing Science* (June 2003) [proceedings.informingscience.org/IS2003Proceedings/docs/063Gani.pdf](http://proceedings.informingscience.org/IS2003Proceedings/docs/063Gani.pdf) accessed 10 March 2008.

<sup>47</sup> See Thara Angskun, Graham E. Fagg, George Bosilca, Jelena Pješivac-Grbović, and Jack J. Dongarra, “Self-Healing Network for Scalable Fault Tolerant Runtime Environments” (University of Tennessee, Knoxville Publication) [www.open-mpi.org/papers/dapsys-2006-self-healing-network/dapsys-2006-self-healing-network.pdf](http://www.open-mpi.org/papers/dapsys-2006-self-healing-network/dapsys-2006-self-healing-network.pdf) accessed 12 March 2008.

<sup>48</sup> For an extensive review of payment and settlement simulations, see Harry Leinonen (ed.), *Liquidity, risks and speed in payment and settlement systems—a simulation approach* (Bank of Finland, 2005), available online at [www.bof.fi/NR/rdonlyres/26D6CF7C-9927-4330-B412-BACDBF50BAAD/0/E31.pdf](http://www.bof.fi/NR/rdonlyres/26D6CF7C-9927-4330-B412-BACDBF50BAAD/0/E31.pdf) accessed 20 March 2008.

<sup>49</sup> U.S. Department of Homeland Security, “Banking and Finance,” 4.

implementing an ACCS system to prevent and respond to gridlock and deadlock in Fedwire. The BCM literature emphasizes that the proper identification of stakeholders is central to the development of any successful plan. Identifying stakeholders guides policy in the same way that identifying operational components guides strategy.

There are several groups of stakeholders regarding the Fedwire network. Firstly, there are the FSS participants, mostly large banks, which make up the nodes of the network. Since this is a very vocal and prominent group, it may be tempting to stop here, and work out policies designed to bolster the security of just this group of stakeholders. In fact, this is what current policy does in many ways, giving banks access to large amounts of liquidity and publicly-funded human resources. Addressing only this group of stakeholders, however, does not produce a comprehensive CIP policy.

When an organization develops a BCM policy, it may first consider its employees and contractors. They are, after all, centrally important to operations. But the chief goal of a policy is to enable the continuity of business operations during a crisis. The organization considers its suppliers and customers, implementing policy to ensure the delivery of goods or services during and after a disaster. These upstream (suppliers) and downstream (customers) elements are essential stakeholder groups. The Banking and Finance CI sector has corresponding stakeholder groups that exist outside of the Fedwire network itself.

Individuals and institutions supply the Fedwire network with the money it uses for daily operations. Individual and institutional “suppliers” provide the money that Fedwire banks transfer. Likewise, individual and institutional “customers” borrow and receive money from Fedwire participants. The daily operations of Fedwire are essentially the movement of money between the accounts of these suppliers and customers. Thus, while the current FSS practices protect the FSS participants through the availability of loans, they do not provide security to the suppliers and customers of the Fedwire network.

But there is another stakeholder, too, that is at least as important in terms of crisis management and CIP. During a financial crisis, the United States government and American public suffers in two major ways. Transactions through financial networks provide revenue to the US and state governments. Capital gains taxes, transactions charges, sales taxes and other various forms of taxation on financial operations provide an important source of public funds<sup>50</sup>. When the Fedwire network is not operating effectively, local, state and federal revenues suffer. This is especially true when there is longer term deadlock or heavy gridlock in the Fedwire network that prevents innumerable taxable transactions from being completed. While it may be impossible to ever precisely gauge the total economic impact of the attacks of 9/11<sup>51</sup>, it is certainly in the many hundreds of billions of dollars<sup>52</sup>.

---

<sup>50</sup> Gerald Auten, “Capital Gains Taxation”, in *Encyclopedia of Taxation and Tax Policy Project*, eds. Joseph J. Cordes, Robert D. Ebel, and Jane G. Gravelle, available online at <http://www.urban.org/UploadedPDF/1000519.pdf> accessed 10 March 2008.

<sup>51</sup> For a review, see Robert Looney, “Economic Costs to the United States Stemming from the 9/11 Attacks,” *Strategic Insights*, Volume 1, Issue 6, August 2002 <http://www.ccc.nps.navy.mil/si/aug02/homeland.pdf> accessed 9 March 2008.

<sup>52</sup> The insurance claim alone was close to \$21 billion according to statistics provided by the reinsurance company Swiss Re at [http://www.swissre.com/INTERNET/pwofilpr.nsf/vwFilebyIDKEYLu/SROS-6MQD65/\\$FILE/F\\_2005.pdf](http://www.swissre.com/INTERNET/pwofilpr.nsf/vwFilebyIDKEYLu/SROS-6MQD65/$FILE/F_2005.pdf) accessed March 9 2008.

During a financial crisis, the public is also impacted by government-sponsored bailouts that use tax revenues to redress operational problems in the financial services. The financial history of the United States has seen the federal government dedicate hundreds of millions of dollars of tax revenue to provide liquidity to FSS participants. While these bailouts have been for the most part effective at restoring the banking and finance system, they are very costly. Most economists agree that bailouts are inefficient and that diverting public funds during financial crises can hurt important civic initiatives such as healthcare and education<sup>53</sup>.

An effective CIP policy should take in to account all of these stakeholder groups and focus also on minimizing the impact on the American public during times of crisis. The Banking and Finance CIP policies in place are concentrated on supporting one stakeholder group, large banks, to the detriment of the overall US financial system and economy. This destructive focus is illustrated in the operation of current gridlock resolution systems. FSS participants give priority to some payments over others, with the goal of settling “higher priority” payments first. The gridlock resolution mechanisms in place today will not settle a group of payments unless these priorities can be satisfied for all banks in the settlement cluster<sup>54</sup>. In general, this results in many fewer settlements, increased delay and a propensity for network gridlock.

Respecting the preferences of banks to settle payments in a specific order is significant to the daily operations of clearing and settlement networks. But during a crisis, deferring to these preferences may make the difference between continuing disaster and a quick resolution. Binding settlement to payment preferences during a crisis upholds the interests of one stakeholder group (private sector FSS participants) while severely disadvantaging the interests of the others (including the federal and states governments, and American public as a whole).

In general, there will be situations where focus must be shifted during times of crisis from one stakeholder group to another. This is a key feature of effective BCM. Businesses will often temporarily inconvenience employees in order to maintain a high level of operation to customers during a crisis. In organizations with well articulated business continuity plans, employees know that putting up with temporary inconveniences (for instance, putting in longer hours) benefits them in the long run because it enables the business to maintain operations. These organizations use a specific set of criteria to determine if and when a business continuity plan will be “activated”, giving a clear signal as to when more focus might be shifted to customers and suppliers.

A convergent CIP policy in the Banking and Finance sector can also provide clear criteria as to when continuity activities will begin, and a well articulated set of activities that will be undertaken to achieve the continuity goals. While the specifics of a convergent CIP policy in the FSS must be developed in conjunction with experienced regulators and financial economists, we can outline the foundations of two broad policy options here.

The first option provides for both path based gridlock resolution (PBGR) and automated liquidity injection from FRB on-demand. Fedwire would operate without the Automatic Cascading Cluster Settlement (ACCS) until an emergency is declared. This

---

<sup>53</sup> For an extensive review, see Benton E. Gup (ed.), *Too Big to Fail: Policies and Practices in Government Bailouts* (Praeger Publishers, 2003).

<sup>54</sup> Bech and Soramäki, “Gridlock Resolution”.



allows FSS participants to keep *all* discretion with regards to payment priorities and taking loans during normal operations (i.e., non-crisis periods). When an emergency is declared, ACCS is activated and remains activated until the emergency is declared over, at which time normal operations are resumed. The first option provides structured response activities, but no preparation over what is currently in practice. Thus it is questionable whether this option meets the goals outlined above.

The second policy option meets both convergent CIP goals of effective preparation and efficient response by providing PBGR at all times. Implementing PBGR during normal operations will drastically reduce the probability of a network gridlock *and* deadlock. It does so, however, by executing sequences of transactions that are efficient for the entire CI/KR sector, and not necessarily the preferences of individual participants<sup>55</sup>. When an emergency is declared, the automated liquidity system is activated on top of PBGR to prevent deadlocks, and it deactivated when the emergency is declared over. This option keeps the operation of all loan activities as they currently are during non-crisis times, allowing banks maximum flexibility during daily operations, and adds an emergency-only liquidity mechanism that quickly and effectively prevents financial disasters from spreading.

The criteria used to declare an emergency will depend on which option is pursued. ACCS will have to be activated more quickly to mitigate a crisis under the first policy option, since there is no intrinsic *protection* against gridlock. This makes option two a much safer choice for the Banking and Finance sector than option one. Under option two, the underlying CI network is *protected* against gridlock and deadlock. Still, it is debatable whether full implementation of an ACCS system during normal operations is a feasible policy option.

The legal and regulatory framework for an automated liquidity system will also depend greatly on what type of policy is pursued. A deciding factor will be the willingness of large banks to participate in the system. Even as the network-wide benefits are clear, it would temporarily inconvenience some FSS participants. The extent of this inconvenience, however, must be weighed against the inconveniences and large-scale problems faced during a financial crisis.

There are three strong and simple arguments that CIP practitioners can make for participation in the automated liquidity system: 1) Involvement in a solid and effective CIP policy will be factored in to the financial markets, reducing perceived volatility. This will reduce the price of money since an effective CIP policy *does* actually increase the stability of US financial markets. 2) The Federal Reserve will be able to lend money using ALLIES at deeply discounted rates over current lending. In an ACCS system, the *minimum* amount of money is spent to resolve network deadlocks, this substantially reduces risks for the FRB *and* saves money for FSS participants. 3) An ACCS system inherently shortens the length of financial crises by implementing the most efficient course back to normal operation, saving money and reducing risks for all groups of stakeholders by addressing the entire Banking and Finance sector holistically.

---

<sup>55</sup> While it would be possible to design a path-based gridlock resolution system that recognizes payment priorities, more research is needed to determine if such a system would present a substantial benefit over the gridlock resolution systems currently in place. The benefit derived from such a system would be largely dependent on other CIP and FSS operational policies in place.

## CONCLUSIONS

The lack of a framework for holistically evaluating critical infrastructure sectors has been a major obstacle to the security community reaching consensus regarding metrics and tools in critical infrastructure protection. While many tools exist for evaluating and comparing single pieces of infrastructure, these tools do not effectively address sector-wide issues at the level of implementation. Traditional reductionist and isolationist methods produce conflict by leading to strategies that many practitioners feel wrongly prioritize some CI elements over others. This is particularly true for CI sectors where the operational elements are less visible, like Banking and Finance.

Recent publications have demonstrated a convergence in thinking and research between critical infrastructure protection and business continuity in the financial services. Both financial economists and security researchers have started emphasizing that *continuity of operations* should be the fundamental goal of CIP in the Banking and Finance, and that the United States clearing and settlement network, Fedwire, should be the focal point of CIP efforts. Here we propose a convergent CIP framework that incorporates principles and methodologies from the area of business continuity management and draws upon current research from the field of network science to design a system of metrics and tools that provides CIP practitioners with a common risk management structure and language.

We apply this convergent framework to the Banking and Finance sector in the form of an intelligent continuity system that works on top of Fedwire. This system meets the goals of the Banking and Finance Sector-Specific Plan, as well as the goals set forth in business continuity literature regarding the financial services by: 1) maintaining a funds transfer network that intrinsically minimizes the probability that clearing and settlement activities will be negatively impacted by outside events, and 2) designing a funds transfer network that quickly and effectively restores clearing and settlement activities between appropriate parties during and after a disaster.

An Automatic Cascading Cluster Settlement (ACCS) system can simultaneously address both of the system-wide risks to Fedwire and the US economy identified by financial economists. *Gridlock* is addressed by an on-demand netting system using Path-Based Gridlock Resolution (PBGR) that investigates payment queues and payment paths in Fedwire. The PBGR algorithm scans the entire network for critical paths and determines the appropriate sequence of payment clusters to solve that allow the greatest percentage of the Fedwire network (i.e., the greatest number of Fedwire participants) to return to normal operation as quickly as possible. PBGR will simultaneously transfer the net amount between all banks in the gridlocked cluster whenever possible, solving one cluster after another unless there is a liquidity shortage, or *deadlock*. The complement to PBGR, an automated liquidity system, solves network deadlocks intelligently alongside PBGR. When ACCS comes across a cluster that cannot be solved by PBGR alone (i.e., netting would result in an overdraft), it identifies the FSS participant where the minimum amount of money must be added to solve the deadlock and any resulting gridlocks, adds this amount to the appropriate account at the FRB and continues the PBGR process.

A convergent strategy provides the security and defense community with a common language and framework, allowing researchers and practitioners from all areas to reach consensus regarding tools and metrics in critical infrastructure protection.

Research in network science, and the extensive literature surrounding business continuity management and continuity of operations, provides a sound and serviceable body of security principles that allow for critical infrastructure protection strategy to be developed and implemented holistically, for entire CI sectors. Conceptualizing sectors as complete entities instead of groups of individual elements allows us to move past the patchwork of strategies and regulations that have become the defining feature of critical infrastructure protection, and develop effective and comprehensive policies for the modern networked infrastructure systems that support the country and connect the world.



# **The Healthcare and Public Health Sector Challenges and Strategies to Conducting Sector Wide Assessments**

Harry Mayer

## ***Introduction***

Our Healthcare and Public Health (HPH) sector is vast, complex and essential to virtually all other sectors of our nation's infrastructure. Without a healthy workforce modern society quickly grinds to a halt. The often messy networks of healthcare providers, insurance companies, emergency departments, pharmaceutical manufacturers and other equally important actors are bound together in fragile alliances to maintain and restore basic health. Thus the HPH sector becomes an important cog in the wheel of infrastructure, if for no other reason than everyone needs healthy workers.

In looking at the HPH Sector as an element of critical infrastructure it is important to note that within the sector there are two very different functions with divergent goals. While healthcare and public health are both in the same sector, they are different disciplines. The fundamental goal of healthcare is to provide medical care to sick or injured patients. The ownership of the subsystems that make up the healthcare system tends to be privately held and is a combination of for profit and not for profit entities. Public health on the other hand, is a government run system. It is not so much concerned with medical care as it is with the health of populations. It seeks out the threats to the population's health and develops intervention strategies to mitigate those threats. The inherent differences between the healthcare and public health systems that comprise the HPH sector make assessment of this sector challenging.

This paper examines the challenges associated with doing a comprehensive assessment of the HPH Sector and then focuses attention on the healthcare system and the hospitals as one of its subsystems. In particular it will discuss how hospitals are intricately linked to other sectors of critical infrastructure. In a modern, technological society, hospitals must depend on services provided by the power, water, energy, information technology/telecommunications (IT/telecom) and transportation sectors. As Hurricane Katrina demonstrated, when key infrastructure sectors in a community fail, a hospital quickly goes from being a center that cares for sick and injured patients to a lifeless facility that can not perform its most basic functions. Part of the challenge during a disaster is the necessity to manage the conflict that arises when services are provided under disaster authorities. In this circumstance there is no charge to patients for government-provided healthcare which can slow recovery by discouraging providers to return to their communities and reopen their practices.

Since hospitals are dependent upon other sectors, preserving their ability to function and treat patients in an all hazard environment becomes a prominent goal of emergency preparedness activities. In this regard, critical infrastructure protection and emergency

preparedness programs have an overlapping interest in promoting resiliency that enables the sector to operate in a multi-threat environment.

### ***Health and Public Health Sector as an element of Critical Infrastructure***

The US Department of Health and Human Services (HHS) has been assigned the responsibility as the nation's sector specific agency for Healthcare and Public Health by Homeland Security Presidential Directive 7 (HSPD 7), and in May of 2007, HHS completed its first sector specific plan. The HPH Sector Specific Plan (SSP) created a framework for integrating Healthcare and Public Health into the National Infrastructure Protection Plan as required by HSPD-7. To accomplish this HHS has created strong public/private partnerships that provide input directly into the HPH SSP through private sector Healthcare Coordinating Councils.<sup>1</sup>

The HPH SSP made tremendous gains in defining the sector and identified areas for future consideration. It also recognized a number of challenges that make a comprehensive nationwide assessment of the sector difficult. This paper will address some of the critical barriers that make sector wide assessments particularly challenging and then proffer a strategy to help mitigate some of these challenges. While this is not an all inclusive list of obstacles these are the issues that make a sector wide assessment particularly thorny, especially if only a top down assessment strategy is followed. The six challenges that will be discussed in this paper are:

- The vastness and complexity of the Healthcare System
- The hierarchal nature of systems
- Organizational differences and variation between public health jurisdictions
- Lack of an agreed upon architecture
- Modeling appropriate relationships
- The ever evolving nature of the Healthcare and Public Health Sector

### ***The Vastness and Complexity of the Healthcare System***

To say that the healthcare system is complex is certainly an understatement. Within the United States there are 13 million health care providers, 6 thousand hospitals, 700 thousand ambulatory care facilities, 6 thousand home healthcare agencies, 70 thousand pharmacies, 170 thousand laboratories and 2 thousand pharmaceutical manufacturers.<sup>2</sup> The vastness and complexity of the healthcare system makes a comprehensive assessment of the HPH Sector extremely challenging. The fact that private ownership of healthcare assets is distributed between the for profit and not for profit portions of the economy, and public health is a government provided service adds to the complexity within the sector.

---

<sup>1</sup> Homeland Security Presidential Security Directive Seven (HSPD-7). 17 December 2003.

<sup>2</sup> US Department of Health and Humans Services. *Public Health and Healthcare Sector Specific Plan; Critical Infrastructure and Key Resources Sector Specific Plan as input to the National Infrastructure Protection Plan (for official use only)*. p-11. May 2007

## *The Hierarchical Nature of Systems*

Practitioners working within the Healthcare and Public Health Sector frequently refer to the sector as a system. But while healthcare seems to meet the definition of a system as discussed in “General System’s Theory” it is not quite as clear with public health.

The principle of “General System’s Theory” as proposed by Ludwig von Bertalanffy in 1931 seems to apply nicely to the healthcare sector and his theory can be used to give us some structure and insight. Bertalanffy, whose work was inspired by the 18<sup>th</sup> Century Gestaltist philosopher Georg Wilhelm Friedrich Hegel was particularly interested in Hegel’s idea, that the whole was more than the sum of the parts. This eventually led to Bertalanffy’s “General System’s Theory”. A biologist by trade, Bertalanffy described systems in terms of supra-systems and subsystems. He believed that a system needed four things in order to exist. It needed parts, elements, or variables; it had to have attributes; and there had to be internal relationships between the components and finally, a system had to exist within an environment.<sup>3</sup>

General System’s Theory describes two types of basic systems. The first was a closed system. A closed system is one that does not interact with its environment. Systems that do not interact with their environment eventually die. The second type of system was an open system. An open system is one that interacts with the environment, it takes inputs from the environment, and it has throughputs and outputs. Hospitals can be viewed as open systems, they take inputs from the community in the form of sick patients, system throughput can be viewed in terms of patient care and finally there are outputs in the form of treated people. But there are other inputs that are necessary to enable a hospital to treat people as well; they need medical supplies (dependent upon the transportation sector); potable water (dependent upon the water sector); electricity (dependent upon the power sector); fuel (dependent upon the energy sector); and communications capabilities (dependent upon the IT/telecom sector). Since several systems are sharing a common environment and all are taking their inputs directly from and sending outputs directly back to the same common environment, each system ends up interacting with the environment in very discrete and complex ways. When we try to apply the “General System’s Theory” definition to public health however; it becomes problematic. Public health can not be easily viewed in terms of inputs and outputs; rather practitioners in the discipline tend to view public health in terms of causation linkages. It is for this reason that this paper is focusing on the healthcare system.

There are times when we want to look at a system in terms of total inputs and total outputs. In these situations we are not necessarily concerned with all of the discrete interactions between the subsystems. This approach, just focusing on the total inputs and outputs is referred to as the black box approach in cybernetics.

---

<sup>3</sup> Littlejohn. *Simple System Model*. Retrieved [http://www.tcw.utwente.nl/theorieenoverzicht/Theory%20clusters/Communication%20Processes/System\\_Theory.doc/](http://www.tcw.utwente.nl/theorieenoverzicht/Theory%20clusters/Communication%20Processes/System_Theory.doc/) 19 Feb 2008.

There are times however, when we are concerned with the interactions between the subsystems. We want to see how one subsystem impacts another. For example at the hospital level we may want to see how the electrical system relates to the water system and the hospitals medical gas distribution system interfaces with other hospital systems. This type of approach is referred to as a white box systems approach.

The inherent nature of systems is that they are hierarchal, the higher you go in the hierarchy the more you must study problems in the abstract. For example, we can view healthcare as a supra-system and hospitals as one of its subsystems. Likewise the hospitals can be viewed as a supra-system and the electrical distribution and supply chain management systems can be seen as subsystems of the hospitals. It is in this sense that systems are hierarchal. While it's possible to study a single hospital and identify multiple vulnerabilities by studying the discrete interaction between its subsystems, as we aggregate this information the ground truth becomes less and less clear. We may see common threads of information and trends between facilities but we can not say with any degree of certainty that these vulnerabilities apply uniformly across the system. One of the lessons learned from Hurricane Katrina was that hospital auxiliary generators and electrical switching rooms are frequently located in basements and while we may be able to make generalized statements that many or most hospitals place their auxiliary generators in basements, it is not a universal truism.

As information about vulnerabilities are rolled up from subsystems to supra-systems the information becomes more abstract and less useful, particularly when it comes to funding specific mitigation projects to eliminate specific vulnerabilities.<sup>4</sup>

### ***Organizational differences and variation in public health jurisdictions***

Adding to the complexity of the HPH sector is the fact that no two public health jurisdictions in the United States are identical. In fact, management of public health through health departments is distributed across 3000 independent city and county health departments and local boards of health, 59 State and territorial health departments, a variety of tribal health departments and 40 different Federal agencies/departments.<sup>5</sup>

There is variation not only in how state health departments are organized but also in the services they deliver. Even within a State there can be considerable differences in how public health services are organized and delivered. In the Commonwealth of Pennsylvania for example, communities are linked to the state health department through six health districts. Each health district is responsible for oversight of six to thirteen counties. The state operates fifty seven health centers and the Pennsylvania Department of Health provides oversight to ten county and municipal health departments that provide service to 40% of the Commonwealth's population.

---

<sup>4</sup> Cybernetics and System Theory, Principia Cybernetica Web; retrieved <http://pespmc1.yub.ac.be/CYBSYSTH.html> 5 Sep 2006

<sup>5</sup> Wasserman, Jeffrey et. Al. *Organizing State and Local Health Departments for Public Health Preparedness*. Prepared by the RAND Center for Domestic and International Health Security for the US Department of Health and Human Services. 2006.



In the five county area that makes up Southeastern Pennsylvania, an area that is made up of a combination of urban, suburban and rural communities there is one city health department, three county health departments and two counties do not have a health department.

Political and economic forces shape health service delivery and the result is a mixed bag of organizations and government provided services. Just as no two states are organized the same, neither are county or municipal health departments. The emergent networks of Healthcare and Public Health creates significant challenges in conducting a meaningful nationwide sector assessment.<sup>6</sup>

### ***Lack of an agreed upon architecture***

Currently there is no universally agreed upon architecture of the HPH Sector, and while the HPH Sector Specific Plan was a good first step in identifying key components of the sector it is far from comprehensive. People who work in the healthcare industry recognize the sector, but there remains no mutually agreed upon architecture.

At HHS the Assistant Secretary for Preparedness and Response (ASPR) has been instrumental in trying to institutionalize the framework and terminology of the HPH Sector. A team of HHS contractors has been mapping the sector and has started to create a framework for a standard taxonomy. While still a work in progress the following taxonomy has started to emerge:

**Sector:** A logical collection of systems, networks, and organizations that provide related goods and services to the economy, government or society (example: Healthcare and Public Health Sector).

**Domain:** A set of services within a sector sharing a common mission or purpose (example: Population Health Management).

**Capability:** The ability to perform designated activities that fulfill a given set of requirements within a sector's domain (example: Surveillance)

**Function:** A set of activities or operations that are carried out to provide sector goods or services (example: Situational Awareness)

**Resource:** A person, asset or material required to perform specified function (Bio Watch Pathogen Sensor)

**External Entity:** An organization outside the sector that provides resources necessary to perform a specified function within the sector (Example: Energy would be

---

<sup>6</sup> Pennsylvania Department of Health. Retrieved <http://www.dsf.health.state.pa.us/health/site/default.asp> 19 Feb 2008

an external entity that supplies the resource of power to a Bio Watch sensor that performs the function of situational awareness).

### ***Modeling appropriate relationships***

One of the beauties of network analysis is its flexibility. Since networks can be depicted as abstract mathematical graphs, it is possible to use them as tools to model a variety of things in the real world. In its most simple form a network map contains two or more nodes that are connected by links, where links represent some type of relationship between the nodes. The user defines the nodes and the links as part of the analytic process. The key to using this methodology effectively is correctly defining the right nodes and right links. Because the HPH Sector is so diverse and complex, it is difficult to find sector wide common denominators.

While it may not be possible to find an appropriate sector wide relationship to model, it should be possible to take one of the sector's domains, such as medical supply chain and model it using network analysis. By limiting the scope to one or two domains the problem becomes less complicated and more meaningful models can be developed thus gaining greater insight into a segment of the sector.

### ***The ever evolving Healthcare and Public Health Sector***

Trends in healthcare delivery continue to shape the HPH Sector, which like most other critical infrastructure sectors continues to emerge. The following is a brief synopsis of some of the major trends that are impacting the sector's evolving structure.

#### 1960-2000

- The percentage of gross national product (GDP) spent on healthcare has increased from 5.1% to 14%

#### 1975-1995

- The national number of acute care hospital beds has declined by 22%
- Hospital admissions have declined by 5%
- The average length of stay per patient has declined by 33%
- Inpatient surgical procedures have declined by 27%

#### 1950-Present

- The number of Americans over 65 years old has tripled and by 2035 this number will increase to approximately 80 million in the United States.

We have also seen a nationwide decline in the number of hospital emergency departments and acute care facilities, while at the same time we have seen increased demand for patients requiring intensive care.<sup>7</sup>

---

<sup>7</sup> Retrieved from <http://www.cdc.gov/ncidod/eid/vol17no2/jarvis.htm> . 15 Feb 2008

We have also seen major changes in healthcare spending. Medicare spending grew at its fastest pace since 1981 due to the new prescription drug plan. Plus we are seeing deceleration in employer payments for health insurance, in part because Medicare is paying a larger share and because private insurance companies are now playing a larger role in Medicare. Since private insurance companies have higher administrative costs less money is being spent on hospitals, doctors and nursing homes.<sup>8</sup>

The impact of these trends means that in the future we will have fewer hospitals with less emergency departments. We can expect to see more and larger intensive care units and greater severity of illnesses in hospitals' inpatient populations. Additionally, we can expect greater reliance on home care, long term care and assisted living.

### ***Mitigating Challenges***

One way to mitigate some of the assessment challenges identified in this paper is to use a risk based approach and focus on one or two domains in a limited geographic area. By taking a system's approach and focusing attention on a portion of the HPH sector we have the luxury of analyzing the discrete interactions between subsystems at the grassroots level, thereby eliminating some of the issues associated with complexity, vastness and jurisdictional variation. By limiting the scope of our assessment, issues such as determining appropriate relationships to model become more workable. Additionally, by keeping within the framework of a defined taxonomy we start to better define the amorphous HPH Sector.

### ***Delaware Valley Model Based Risk Analysis Project (Del Val MBRA Project)***

At this time there is no widely accepted, probability based risk assessment methodology that assesses the impact of a large scale disaster on a hospital. Over the years several different assessment tools have been developed, but most fall short of meeting the National Infrastructure Protection Plan's baseline criteria for risk calculus (Risk = Consequences \* Vulnerabilities \* Threat).<sup>9</sup>

The Delaware Valley, a densely populated area that covers Southeastern Pennsylvania, Northern Delaware and Southern New Jersey is an ideal location to conduct a limited study of the Direct Patient Services and Medical Supply Chain Domains. The Region contains a mix of urban, suburban and rural communities with a large concentration of tertiary hospital beds, Healthcare is currently one of the largest industries in Southeastern Pennsylvania and the area is particularly known to have one of the most competitive healthcare markets in the nation.

The US Department of Health and Human Services (HHS) is participating in a study with the Delaware Valley Healthcare Council (DVHC) (the areas local hospital association) to conduct the first field test of Model Based Risk Analysis (MBRA) in the HPH Sector. After benchmarking several other critical infrastructure protection

---

<sup>8</sup> Pear, Robert. *Health Spending Exceeded Record \$2 Trillion in 2006*, *NY Times*. 8 Jan 2008

<sup>9</sup> U. S. Department of Homeland Security, *National Infrastructure Protection Plan*. P.36. 2006

methodologies, MBRA was selected as the methodology of choice because it was the closest in meeting the NIPP's baseline criteria for risk calculus. This project is limiting its scope of work to look specifically at hospitals as a subsystem of the healthcare system in a defined geographic region.

The elements of risk calculus for this project are defined as follows:

$$\text{Risk} = \text{Consequences (C)} * \text{Vulnerabilities (V)} * \text{Threat (T)} \quad [R=C*V*T]$$

Consequences (C) are defined as a hospital's loss of functions due to an adverse event generated by the exploitation of vulnerabilities. Downstream consequences associated with specific vulnerabilities plays a vital role in risk management calculations.

Vulnerabilities (V) are defined as weaknesses that would degrade hospital functions. These vulnerabilities include key dependencies on: power (p); water (w); energy (e); IT/Telecom (i) and transportation (t)

Threat (T) is defined as the likelihood that any of these key dependencies would be interrupted:  $[T=p*w*e*i*t]$ .

The Del Val MBRA Project will study five different hospitals in the Delaware Valley and examine the discrete interactions between the subsystems using fault and event tree analysis. The purpose of using fault/event trees will be to identify specific vulnerabilities and specific losses of hospital functions (consequences) caused by a disaster that disrupts services in the following sectors: power (p), water (w), energy (e), IT/telecom (i) and transportation (t). Additionally, through network analysis the project will examine the medical supply chain and the impact that disruption of services from  $p*w*e*i*t$  will have on the five selected hospitals. While the project is still in its infancy, the following is a statement of the project's goal, objectives, expected outcomes and potential benefits.

**Project Goal:** The project's goal is to improve hospital survivability and enhance the HPH sector's resilience in an all hazard threat environment.

**Objective:** To field test Model Based Risk Analysis methodology and determine its applicability to the HPH Sector as a means to improve hospital survivability and enhance the healthcare sector's resiliency in an all hazard threat environment.

**Expected Outcome #1:** Determine critical distributors and suppliers in the medical supply chain through network analysis

**Expected Outcome #2:** Use fault and event tree analysis to identify major weaknesses (vulnerabilities) of a hospital

**Expected Outcome #3:** Identify the most significant functions (consequences) that are lost when dependent sectors are compromised

Expected Outcome #4: Determine the most appropriate resource allocation strategy to mitigate risk

Potential Benefit: The movement of hospital patients either before or after a disaster exposes them to increased harm and will likely result in unnecessary deaths. By developing a risk based approach to hospital resiliency and risk mitigation it is possible to engineer disaster resilient hospitals that can deliver patient services in an all hazards environment.

### Conclusion

In conclusion, the inherent differences between healthcare and public health, both in their goals and how they deliver their services causes significant problems in conducting a comprehensive sector assessment. When healthcare services are delivered in an all hazard environment there is an inherent need to balance patient services with business functions. During disasters there is a general expectation that hospitals should provide services for the public good regardless of an individual's ability to pay, yet providing such services could compromise the financial viability of the institution. This presents natural conflict between the public and the private sectors.

There has been a considerable collaboration between the public and private sectors through the Healthcare Coordinating Council to define a path ahead to protect HPH Sector. Despite these gains the issues of:

- Vastness and complexity of the healthcare system
- The hierarchal nature of systems
- Organizational differences and variation in public health jurisdictions
- Lack of an agreed upon architecture for the sector
- Modeling appropriate relationships
- Ever emerging health and public health sector

create systemic problems that make a top down comprehensive assessment of the sector impractical. While a top down assessment of the HPH Sector may not be practical, a bottom up strategy that looks at specific subsystems within a limited geographic area can be useful. By following a bottom up strategy we can gain greater knowledge of the discrete interactions that take place between subsystems in the larger Healthcare System and in doing so uncover weaknesses and vulnerabilities that may have otherwise gone unnoticed. By using a sound risk based assessment methodology, funds can be better targeted to mitigate risk and build appropriate redundant systems that will allow facilities to withstand the challenges of an all hazard threat environment. By increasing a hospitals ability to continue to function and bill for services throughout a disaster it will be possible to lessen the inherent conflict between the public and private sectors during future disasters.

DHHS 3/25/08 8:32 AM  
Deleted: s

DHHS 3/25/08 8:33 AM  
Deleted: s

DHHS 3/25/08 8:33 AM  
Deleted: government

DHHS 3/25/08 8:34 AM  
Deleted:

DHHS 3/25/08 8:35 AM  
Formatted: Bullets and Numbering

DHHS 3/25/08 8:36 AM  
Deleted: v

DHHS 3/25/08 8:35 AM  
Deleted: , the

DHHS 3/25/08 8:37 AM  
Deleted: , o

DHHS 3/25/08 8:37 AM  
Deleted: ,

DHHS 3/25/08 8:37 AM  
Deleted: l

DHHS 3/25/08 8:37 AM  
Deleted: ,

DHHS 3/25/08 8:37 AM  
Deleted: modeling appropriate relationships and the

DHHS 3/25/08 8:38 AM  
Deleted: e

DHHS 3/25/08 8:38 AM  
Deleted: nature of the

DHHS 3/25/08 8:38 AM  
Deleted: HPH

DHHS 3/25/08 8:39 AM  
Formatted: Indent: Left: 0.5"



## HOW MUCH AND ON WHAT?

Robert Powell\*

March 2008

### Abstract:

How much should a defender spend on defense and how should it allocate those resources across the sites it is trying to protect? This paper analyzes a model in which a defender first has to decide how much to spend on defense and what to spend it on. The more that a defender devotes to protecting a specific site, the less likely an attack on that site is to succeed and, crucially, the lower the marginal return to investing in attacking that site. After the defender moves, the attacker decides how much effort to devote to attacking each site. Three key conclusions result: First, the questions of how much to spend and what to spend it on are “separable.” However much the defender decides to spend, it should allocate those resources in the same general way. Second, a very simple principle or algorithm determines the optimal allocation. The defender *minmaxes* the attacker’s marginal gains, i.e., allocates its resources in the way that minimizes the attacker’s maximum marginal gain from exerting additional effort. Third, the defender is in effect a Stackelberg leader. The optimal level of spending takes into account how the defender’s allocation affects the attacker’s effort and generally is that level of spending which equates the marginal benefits of additional spending with the marginal cost of diverting these resources from other social ends.

\* Travers Department of Political Science, 210 Barrows Hall, UC Berkeley Berkeley, CA 94720-1950 (R.Powell@Berkeley.edu).

## HOW MUCH AND ON WHAT?

Two factors make the problem of defending against terrorists especially daunting. First, as the *National Strategy for Homeland Security* emphasizes, “terrorists are strategic actors” (White House 2002, 7). No one believes that hardening the levies around New Orleans affects the probability that another hurricane like Katrina will strike New Orleans again or Miami rather than New Orleans. But strategic actors do try to strike where the defense is weak and the expected gains are high. Protecting one site may shift the risk of attack to another. “Increasing the security of a particular type of target, such as aircraft or buildings, makes it more likely that terrorists will seek a different target. Increasing countermeasures to a particular terrorist tactic, such as hijacking, makes it more likely that terrorists will favor a different tactic” (White House 2002, 29).

Second, relative to the large number of potential targets, resources are scarce. We cannot defend everything. As Department of Homeland Security Secretary Michael Chertoff assessed the situation shortly after taking office, “Although we have substantial resources to provide security, these resources are not unlimited. Therefore, as a nation, we must make tough choices about how to invest finite human and financial capital to attain the optimal state of preparedness” (2005b). Echoing the *9/11 Commission*, Secretary Chertoff has emphasized throughout his tenure that these scarce resources should be allocated on the basis of risk. “Risk management must guide our decision making as we examine how we can best organize to prevent, respond and recover from an attack” (2005a).

This paper offers a game-theoretic framework for analyzing two related questions. How much should a defender spend on defending against a strategic attacker, i.e., a terrorist group, instead of devoting those resources to other social ends like health care or education? Second, how should a defender allocate however much it decides to spend among the multiple sites it is trying to protect?

In the model, a defender first has to decide how much to spend on defense and what to spend it on. The more that a defender devotes to protecting a specific site, the less likely an attack on that site is to succeed and, crucially, the lower the marginal return to investing in



attacking that site. After the defender moves, the attacker decides how much effort to devote to attacking each site. In order to focus on the fundamental ideas, insights, and intuitions, we simplify matters by assuming that all of the sites the defender is trying to protect are identical. But the results generalize to a setting in which some or all of the sites differ from others.

Three key conclusions follow from the analysis. First, the questions of how much to spend and what to spend it on are “separable.” However much the defender decides to spend, it should allocate those resources in the same general way.

Second, a very simple principle or algorithm determines the optimal allocation. Suppose that the defender has decided to spend a specific amount on defense but has not yet allocated it. Given this null allocation, a strategic attacker will direct its efforts to the site offering the highest marginal return on that effort. The defender therefore should invest in hardening this site and reducing the attacker’s expected return from trying to attack it. The more the defender spends on this site, the less vulnerable it becomes and the lower the expected return to an attack. Eventually, this site will be no more attractive than what was initially the second most attractive site. That is, both offer the same marginal return on the attacker’s effort to strike them. At this point, the defender must invest in protecting both sites so the neither is more attractive than the other. The more the defender spends on these two sites, the lower their vulnerability and the less attractive targets they become. At some point, these sites are no more attractive than what was originally the third most attractive site. From here on the defender must invest in guarding all three sites so that that no one site is any more attractive than the other two. The defender continues to allocate its resources in this way by spending so as to make the most attractive profile as unattractive as possible. In brief, the defender *minmaxes* the attacker’s marginal gains, i.e., allocates its resources in the way that minimizes the attacker’s maximum marginal gain from exerting additional effort.

The third conclusion is that the defender is in effect a Stackelberg leader. The optimal level of spending takes into account how the defender’s allocation affects the attacker’s effort and generally is that level of spending which equates the marginal benefits of additional spending with the marginal cost of diverting these resources from other social ends. In principle, the defender may be able to spend enough to induce the attacker to exert zero effort in carrying out an attack. But this may require such a high level of defense spending that it is not optimal.

The next section presents the game-theoretic model. It also links the basic components of the model to the critical elements of risk management, consequence, vulnerability, and threat. The subsequent section characterizes the defender's optimal level of spending and the attacker's optimal level of effort. There follows a discussion of the comparative statics describing how the optimal levels of spending and effort change as the underlying parameters change. The last section discusses the generality of the results and an appendix sketches a game-theoretic analysis of the model.

## A Model

A defender has  $N$  identical sites to protect and must decide how much to spend on defending them and how to distribute those resources across the sites it is trying to guard. The more the defender dedicates to a given site, the "harder" that site becomes and the less likely an attack on that site is to succeed. After observing the defender's allocation, an attacker decides how much effort to devote to attacking each site. The more effort the attacker devotes to striking a specific site, the more likely the attack on that site is to succeed.

A strategy for the defender in this game simply specifies how much the defender spends on each site. In symbols, it is an allocation  $r = (r_1, \dots, r_N)$  where  $r_j \geq 0$  is the amount allocated to site  $j$ . The total spent on defense is implicitly defined by  $R = \sum_{j=1}^N r_j$ . Analogously, the attacker's strategy specifies how much effort it will put into attacking each site after observing any possible allocation  $r$ . More precisely, a strategy for the attacker is a function  $e(r) = (e_1(r), \dots, e_N(r))$  where  $e_j(r) \geq 0$  is the effort the attacker puts into striking site  $j$ .

Let  $\lambda > 0$  denote the loss the defender suffers if a site is successfully attacked. If the attack fails, the defender's loss is zero. (We assume for simplicity that an attack either succeeds or fails.) The attacker gains of  $\gamma > 0$  if a site is successfully attacked and zero if the attack fails.

The more the defender spends on a site, the less likely an attack on that site is to succeed. Formally, let  $V_j(r_j, e_j)$  be the probability that an attack on site  $j$  succeeds if the defender spends  $r_j$  on hardening that site and the attacker expends effort  $e_j$  on hitting that site.  $V_j(r_j, e_j)$  is increasing in  $r_j$  and decreasing in  $e_j$ .

We now make an important assumption which greatly simplifies the analysis. The vulnerability of a site is multiplicatively separable in effort. That is, we can write the vulnerability  $V_j$  as  $V_j(r_j, e_j) = v_j(r_j)e_j$  where the function  $v_j$  depends solely on  $r_j$ . The substantive significance of this assumption is that the marginal effect of additional effort on the vulnerability of a site is independent of the level of effort already being exerted. That is,  $\partial V_j / \partial e_j$  is independent of  $e_j$  or  $\partial^2 V_j / \partial e_j^2 = 0$ . Stating this assumption more formally:

ASSUMPTION 1 (SEPARABILITY): *The vulnerability of each site  $j$  can be written as  $V_j(r_j, e_j) = v_j(r_j)e_j$ .*

Assumption 1 is critical to the analysis. A second simplifying assumption makes the algebra easier but is not substantively critical. We assume the  $v_j$  is linear in resources, i.e.,  $v_j(r_j) = 1 - vr_j$ . If the defender devotes nothing to site  $j$ , then  $r_j = 0$ ,  $v_j(0) = 1$ , and an attack on this site is sure to succeed. The parameter  $v$  measures the marginal effect that additional resources have on the vulnerability of a site. The larger  $v$ , the greater the effect of additional spending on the vulnerability of a site.<sup>1</sup>

Spending on defense means diverting resources from other social ends. These costs are assumed to rise and at an increasing rate as  $R$  increases. More concretely, let take the cost to devoting  $R$  to defense to be  $c_D(R) = k_D R^2$ . The parameter  $k_D$  measures the social opportunity cost of spending on defense rather than some other social goal. The higher  $k_D$ , the more costly defense is relative to other social priorities and the faster these costs rise as  $R$  increases.

Resource are scarce for the attacker too. Let  $E = \sum_{j=1}^N e_j$  denote the total effort expended on attacking. Then the cost of exerting this effort is assumed to be  $c_A(E) = k_A E^2 / 2$  where  $k_A$  measures the relative difficulty the attacker has in exerting the effort needed to carry out an attack.

---

<sup>1</sup> We assume  $v$  is small enough that  $v_j(r_j) > 0$  over the substantive relevant range of resource allocations.

In light of all of this, the defender's expected loss if it allocates  $r$  and the attacker replies with  $e(r)$  is  $L(r, e(r)) = \sum_{j=1}^N \lambda v_j(r_j) e_j(r) + c_D(R)$ . The attacker's payoff is

$$G(r, e(r)) = \sum_{j=1}^N \gamma v_j(r_j) e_j(r) + c_A(E).$$

The basic elements of this model broadly correspond to the three key components of risk-management which are vulnerability, threat, and consequence. Vulnerability "is the probability that a particular attack will succeed against a particular target" (GAO 2005, 25), and this is what  $v_j(r_j)$  is in the model. Threat "is the probability that a specific target is attacked in a specific way" (Willis et. al. 2005, 8). In this formulation, the amount of effort the attacker puts into hitting a site serves as a proxy for the probability of an attack on that site. Finally,  $\lambda$  formalizes the defender's "range of loss or damage that can be expected from a successful attack" (NIPP 2006a, 41).<sup>2</sup>

Note, however, that nothing in the risk-management framework corresponds to the cost of spending on defense rather than something else, i.e., nothing corresponds to  $c_D(R)$  in the model. At its best, risk-management provides guidance on how one should allocate a fixed amount of resources. It says little or nothing about how to determine the optimal amount to spend on defense.

### The Optimal Levels of Resources and Effort

This section describes the intuitions underlying the equilibrium outcome. The appendix offers a more detailed game-theoretic discussion of the equilibrium. The fact that the sites are identical suggests the defender will distribute however much it decides to spend evenly across the  $N$  sites. In symbols,  $r_j = R/N$ . This leaves the defender with losses of

$$L = \sum_{j=1}^N \lambda [1 - vR/N] e_j + c_D(R) = \lambda [1 - vR/N] \sum_{j=1}^N e_j + c_D(R) = \lambda [1 - vR/N] E + c_D(R). \text{ The}$$

---

<sup>2</sup> Strictly speaking,  $\lambda$  is a von Neumann-Morgenstern utility which is related to economic losses but is not the same thing.

attacker's payoffs are  $G = \sum_{j=1}^N \gamma [1 - vR/N] e_j + c_A(E) = \gamma [1 - vR/N] E - c_A(E)$ . Note that the only choice left to determine is how much the defender spends and level of effort  $E$ .

The defender will choose  $R$  partly based on the defender's anticipation of how the attacker will react. To determine this, consider the attacker's decision after seeing that the defender has allocated  $R$  to defense and spread these resources evenly across the  $N$  sites. The attacker chooses  $E$  to maximize its gain  $G$  given this allocation. Taking the derivative of  $G$  with respect to  $E$  and setting it equal to zero gives the first-order condition:

$$0 = \frac{\partial G}{\partial E}$$

$$0 = \gamma \left[ 1 - \frac{vR}{N} \right] - k_A E$$

$$E = \frac{\gamma}{k_A} \left[ 1 - \frac{vR}{N} \right]$$

where recall  $c_A(E) = k_A E^2 / 2$ .<sup>3</sup> Thus, for any given allocation  $R$ , the attacker's optimal level of effort is  $E^*(R) \equiv (\gamma / k_A) [1 - vR/N]$ . This level of effort equates the marginal gain from additional effort,  $\gamma [1 - vR/N]$ , with the marginal cost  $c'_A(E) = k_A E$  (see the second equality above). As expected, there is an inverse relation between the defender's spending and the attacker's effort. As  $R$  increases,  $E^*(R)$  declines.

The function  $E^*(R)$  describes how the attacker alters its level of effort in response to varying levels of defense spending. Anticipating that the attacker will respond in this way, the defender's losses to  $R$  are  $L = \lambda [1 - vR/N] E^*(R) + c_D(R)$ . The optimal allocation  $R$  minimizes these losses. To solve for this, differentiate  $L$  with respect to  $R$  to obtain:

---

<sup>3</sup> This critical point is sure to maximize  $G$  since  $\partial^2 G / \partial E^2 = -k_A < 0$ .

$$\frac{\partial L}{\partial R} = \underbrace{\frac{\partial \lambda [1 - vR/N]}{\partial R} E^*(R)}_{\text{defensive effect of increasing } R} + \underbrace{\lambda [1 - vR/N] \frac{\partial E^*(R)}{\partial R}}_{\text{deterrent effect of increasing } R} + \underbrace{c'_D(R)}_{\text{cost effect of increasing } R}$$

The expressions on the right side of this equality offer a useful decomposition of the effects of an increase in defense spending into the *defensive effect*, the *deterrent effect*, and the *cost effect*. The first term, the defensive effect of an increase in  $R$ , is the effect that spending more on hardening the sites has on the defender's expected losses *given that the attacker's level of effort remains the same*. The second term might be thought of as the deterrent effect. This is the decrease in the defender's losses resulting from the attacker's decision to invest less effort in mounting an attack. Finally, the third term is the increase in losses due to the greater expenditure on defense.

Substituting the expressions for  $E^*(R)$  and  $c_R(R)$  and then solving for the optimal allocation  $R^*$  gives:<sup>4</sup>

$$R^* = \frac{\gamma \lambda v N}{\gamma \lambda v^2 + k_A k_D N^2}.$$

This then implies that the optimal level of effort  $E^*(R^*)$  is

$$E^* = \frac{\gamma k_D N^2}{\gamma \lambda v^2 + k_A k_D N^2}$$

The defender's losses are:

$$L^* = \frac{\gamma \lambda k_D N^2}{\gamma \lambda v^2 + k_A k_D N^2}.$$

---

<sup>4</sup> This critical point is sure to minimize  $L$  since  $\partial^2 L / \partial R^2 > 0$ .

In sum, when the defender anticipates how the attacker responds to the defender's actions, the optimal level of spending is  $R^*$ , the attacker exerts  $E^*$ , and the defender's expected loss is  $L^*$ .

### Comparative Statics

How do the optimal level of spending and the defender's losses vary with the parameters of the model? Suppose, for example, that the opportunity cost of spending on defense increases (i.e.,  $k_D$  goes up). This makes defense spending more costly and, intuitively, seems likely to result in lower spending and higher losses. Moreover, these higher losses will be due in part to the fact that the attacker will exert more effort to carrying out an attack. Formally, the effect of an increase in  $k_D$  on  $L^*$  is:

$$\frac{\partial L^*}{\partial k_D} = \underbrace{\frac{\partial \lambda [1 - vR^* / N]}{\partial k_D} E^*}_{\text{direct effect on losses from an attack due to lower spending}} + \underbrace{\lambda [1 - vR^* / N] \frac{\partial E^*}{\partial k_D}}_{\text{indirect effect on losses from an attack due to changes in effort}} + \underbrace{\frac{\partial c_D(R^*)}{\partial k_D}}_{\text{cost effect of } k_D}$$

Inspection of the expression for  $R^*$  shows that the level of defense spending decreases as the cost of diverting those resources from other social purposes  $k_D$  increases ( $\partial R^* / \partial k_D < 0$ ). Hence the direct effect of an increase in  $k_D$  is positive. Spending goes down, sites are not more vulnerable, and the defender's losses from an attack rise.

The same is true of the indirect effect. As  $k_D$  increases, the defender's spending decreases, and this induces the attacker to increase its effort  $E^*$ . Finally, the cost effect by itself is ambiguous as a larger  $k_D$  makes any given level of spending more costly but the higher  $k_D$  also reduces the level of spending  $R^*$ . Nevertheless, the first two effects swamp the potentially ambiguous third effect and the defender's losses increase as  $k_D$  increases (the expression for  $L^*$  is clearly increasing in  $k_D$ ).

Similarly, the defender's losses are increasing in (i) the losses  $\lambda$  the defender suffers if a site is destroyed, (ii) the gains  $\gamma$  the attacker gets from destroying a site (since this induces greater effort), and (iii) the number of sites  $N$ . Defense spending  $R^*$  is increasing in the gains  $\gamma$  and losses  $\lambda$ . It decreases as the costs  $k_A$  and  $k_D$  rise. Finally, the attacker's effort is increasing in the attacker's gains  $\gamma$  and decreasing in its costs  $k_A$ .

### Some Generalizations

The formal analysis has centered on a model in which the sites are identical. But many of the results generalize beyond this. The critical assumption is the separability assumption which recall is that the vulnerability of every site  $j$  can be written as  $V_j(r_j, e_j) = v_j(r_j)e_j$ . As long as this holds, the results go through.<sup>5</sup> More precisely, let  $\lambda_j$  and  $\gamma_j$  be the defender's loss and the attacker's gain if site  $j$  is successfully attacked. Then the results described above hold even if these losses and gains differ across the sites (i.e.,  $\lambda_j$  need not equal  $\lambda_k$  and  $\gamma_j$  need not equal  $\gamma_k$ ), the defender's losses differ from the attacker's gain (i.e.,  $\lambda_j$  need not equal  $\gamma_k$ ), and the functions relating vulnerability to resources,  $v_j(r_j)$ , differ from site to site.<sup>6</sup>

To outline the analysis in the more general case, recall that the marginal return the attacker obtains from investing effort in attacking site  $j$  is  $\gamma_j v_j(r_j)$ . Thus the attacker will only invest effort in attacking the sites offering the highest return on this investment, namely those sites  $k$  such that  $\gamma_k v_k(r_k) = \max\{\gamma_j v_j(r_j)\}$ . Given that the marginal return to effort is  $\max\{\gamma_j v_j(r_j)\}$ , the attacker exerts the level of effort  $E^{**}$  that equates the marginal return on this

---

<sup>5</sup> Some mild technical assumptions are also needed. The loss function  $L$  is kinked and possibly discontinuous at finitely many value of  $R$ . The needed technical conditions ensure that  $\partial^2 L / \partial R^2 > 0$  everywhere else.

<sup>6</sup> See Powell (2008) for an analysis of a more general game that allows each site to differ from the others. The attacker in Powell's model chooses the probability of attacking rather than the level of effort. But the separability assumption ensures that these two formulations are essentially equivalent.



effort to the marginal cost, i.e.,  $\max\{\gamma_j v_j(r_j)\} = c'_A(E^{**})$ . It follows that if the defender decides to spend  $R$  on defense, it will allocate those resources so as to minimize the attacker's maximum marginal return to effort. That is, the defender distributes  $R$  in the way that minimizes  $\max\{\gamma_j v_j(r_j)\}$ . The defender now chooses the allocation  $R$  that minimizes the defender's losses in light of this reaction.

## Conclusions

The *National Strategy for Homeland Security* emphasizes that terrorists are strategic, and this poses at least two questions. When allocating scarce resources to defend against strategic attacker's, how much should the defender spend on defense and how should it allocate those resources across the sites it is trying to protect? Strategic interaction often makes resource-allocation problems extraordinarily difficult to analyze, but that turns out not to be the case here. Taking the effects of strategic interaction is relatively straightforward and yields three key findings.

First, the defender's level and allocation problems are separable. However much the defender decides to spend, it should allocate those resources in the same general way. Second, the defender should allocate however much it decides to spend so as to minmax the attacker's return on its effort. Finally, the defender's strategic position is analogous to that of a Stackelberg leader. Taking into account how the defender's allocation will affect the attacker's effort, the optimal level defense spending generally equates the marginal benefits of additional spending with the marginal cost of diverting these resources from other social ends.

## Appendix

This appendix sketches a game-theoretic analysis of the model. A subgame perfect equilibrium is a strategy profile  $(r^*, e^*(r))$  such that (i) the effort allocation  $e^*(r)$  maximizes the attacker's payoff  $G(r, e(r)) = \sum_{j=1}^N \gamma[1 - vr_j]e_j(r) + k_A E^2 / 2$  for every resource allocation  $r$ , and (ii) the resource allocation  $r^*$  minimizes the defender's loss

$$L(r, e(r)) = \sum_{j=1}^N \lambda[1 - vr_j]e_j(r) + k_D R^2 \text{ given that the attacker plays according to } e^*(r).$$

Solving the game by starting with the last decision and working up the game tree to the first decision, consider the attacker's decision following any allocation  $r$ . It wants to choose  $e_j$  so as to maximize  $\sum_{j=1}^N \gamma[1 - vr_j]e_j + k_A E^2 / 2$  where  $E = \sum_{j=1}^N e_j$ . The separability assumption plays a crucial role at this point. Given that the attacker's marginal return to increasing  $e_j$ , i.e.,  $\gamma[1 - vr_j]$ , is independent of  $e_j$ , this maximization problem has a very simple solution.

The attacker will only invest effort in the site or sites offering the highest marginal return on that investment. That is, the attacker will only invest effort in going after  $k$  if  $\gamma[1 - vr_k] = \max\{\gamma[1 - vr_j] : j = 1, \dots, N\}$ . Let  $T(r)$  denote the set of the sites offering the attacker its highest expected marginal return:  $T(r) = \{k : \gamma[1 - vr_k] = \max\{\gamma[1 - vr_j] : j = 1, \dots, N\}\}$ . Then the attacker invests no effort in attacking sites outside  $T$ , i.e.,  $e_i = 0$  for  $i \notin T(r)$ . This implies that the attacker's payoff reduces to:

$$\begin{aligned} G(r, e(r)) &= \sum_{k \in T(r)} \gamma[1 - vr_k]e_k - \frac{k_A E^2}{2} \\ &= \gamma[1 - vr_k] \sum_{k \in T(r)} e_k - \frac{k_A E^2}{2} \\ &= \gamma[1 - vr_k]E - \frac{k_A E^2}{2} \end{aligned}$$

where the second line follows from the first because  $\gamma[1 - vr_k] = \gamma[1 - vr_j]$  for all  $j, k \in T(r)$ .

Differentiating the previous expression with respect to  $E$  yields shows that the optimal level of effort given allocation any  $r$  is  $E^*(r) = (\gamma / k_A)[1 - vr_k]$  where  $k$  is any element in  $T(r)$ . If there are two or more sites that offer the maximum return on the attacker's effort, i.e., if  $T(r)$  contains two or more sites, the allocation  $E^*(r)$  across the sites in  $T(r)$  is arbitrary because the return on every allocation is the same. Since the attacker's allocation across the sites in  $T(r)$  is arbitrary, let  $t(r)$  be the site in  $T(r)$  with the smallest index, that is,  $t(r) = \min\{j : j \in T(r)\}$ , and suppose that the attacker allocates all of  $E^*(r)$  to  $t(r)$ .

Turning to the defender's strategy, the problem for the defender is to select the allocation  $r^* = (r_1^*, \dots, r_N^*)$  given the attacker's strategy of allocating  $E^*(r)$  to  $t(r)$ . Formally, the defender wants to choose  $r^*$  to minimize  $L(r, e^*(r)) = \lambda[1 - vr_{t(r)}]E^*(r) + k_D R^2$ . This is equivalent to selecting the allocation  $r$  that solves  $\min_r \{ \max_{j=1, \dots, N} \{ (\lambda\gamma / k_A)(1 - vr_j)^2 \} + k_D R^2 \}$ . Because all of the sites are identical, the minmax allocation of  $R$  is to distribute  $R$  evenly across the  $N$  sites. That is, the optimal distribution of  $R$  is to set  $r_j = R / N$ . This means that the defender's losses reduce to  $(\lambda\gamma / k_A)(1 - vR / N)^2 + k_D R^2$ . Differentiating with respect to  $R$  yields the optimal allocation  $R^* = \gamma\lambda vN / (\gamma\lambda v^2 + k_A k_D N^2)$ .

In sum, the subgame perfect equilibrium allocation entails a level of spending  $R^*$  spread evenly across the  $N$  sites. The attacker's total level of effort is  $E^*(R^*) = \gamma k_D N^2 / (\gamma\lambda v^2 + k_A k_D N^2)$ .

## References

- 9/11 Commission Report. 2003. *Final Report of the National Commission on Terrorist Attacks upon the United States*, New York: Norton.
- Chertoff, Michael. 2005a. "Remarks for Secretary Michael Chertoff U.S. Department of Homeland Security George Washington University Homeland Security Policy Institute," Washington, DC Department of Homeland Security, March 16. Available at [www.dhs.gov/dhspublic/display?content=4391](http://www.dhs.gov/dhspublic/display?content=4391).
- Chertoff, Michael. 2005b. "Secretary Michael Chertoff U.S. Department of Homeland Security Second Stage Review Remarks." Washington, DC: Department of Homeland Security, July 13. Available at [www.dhs.gov/dhspublic/display?content=4597](http://www.dhs.gov/dhspublic/display?content=4597).
- GAO. 2005. "Risk Management." Washington, DC: Government Accountability Office. Available at: [www.gao.gov/cgi-bin/getrpt?GAO-06-91](http://www.gao.gov/cgi-bin/getrpt?GAO-06-91).
- NIPP. 2006. DHS. "Draft National Infrastructure Protection Plan, v2.0." Washington, D.C.: Department of Homeland Security. Available at: [www.fas.org/irp/agency/dhs/nipp110205.pdf](http://www.fas.org/irp/agency/dhs/nipp110205.pdf).
- Powell, Robert. 2008. "Defending Against Strategic Attackers: Deciding How Much to Spend and on What," Manuscript, Department of Political Science, UC Berkeley.
- White House. 2002, "National Strategy for Homeland Security." Washington, DC: White House, July. Available at [www.whitehouse.gov/homeland/book/index.html](http://www.whitehouse.gov/homeland/book/index.html).
- Willis, Henry H., Andrew R. Morral, Terrance K. Kelly, and Jamison J. Medby. 2005. *Estimating Terrorism Risk*. Santa Monica, CA: Rand Corporation.



# Security Risk Management: Implementing a National Framework for Success in the Post 9-11 World

*Edward J. Jopeck, President  
Security Analysis and Risk Management Association*

*Kerry L. Thomas, Executive Vice President  
Security Analysis and Risk Management Association*

---

Over the past several decades, significant resources have been expended by Federal departments and agencies to implement more uniform and rigorous security risk management processes and methods. However, despite the considerable sums spent to affect change, security risk management efforts across the Federal government have remained at roughly the same level in terms of sophistication, coordination and comparability as they were more than a decade ago. Furthermore, while some of these efforts have sought to dictate “standards” for government-wide use, none have gained significant acceptance outside of the organizations where they originated.

The terrorist attacks of September 11, 2001, and the subsequent creation of the Department of Homeland Security (DHS), have added a further degree of complexity to this issue. In addition to large numbers of new security risk analysis users, the focus on homeland security that emerged in the wake of these attacks also imbued security risk management efforts with significant sums of new money. DHS and other Federal agencies have used the new funding to develop and implement a variety of security programs, many of which rely on risk management principles as a key part of their decision framework. Despite this, the numerous directives and plans arising out of the homeland security enterprise either disseminate conflicting guidance or remain silent on risk management methods that should be employed to achieve comparable results. As a result, more than six years after 9/11, the Nation has not yet achieved a consistent, risk-based approach that provides decision-makers at all levels measurable results for intelligently reducing terrorist risks.

In the post 9/11 security environment, where the price of failure in both lives and dollars can be staggering, few can argue about the role of risk management or the urgency of overcoming the challenges to using it effectively. Just as the 9/11 Commission identified emergency responder radio interoperability as a critical shortfall, clear guidance on “interoperable” risk analysis approaches is also needed to permit effective risk communication between homeland security organizations with similar missions. This article attempts to identify the primary reasons for this apparent lack of progress, and explores a vision for implementing a more successful risk management program that can provide the Nation the security it needs at a price it can afford.

## Identifying the Problems

While there is virtually no disagreement over the need to use risk as a decision support tool for homeland security activities, prior attempts to do so have failed largely because they did not address the fundamental building blocks needed to establish the basis for success. Figure 1 below illustrates this in more detail.

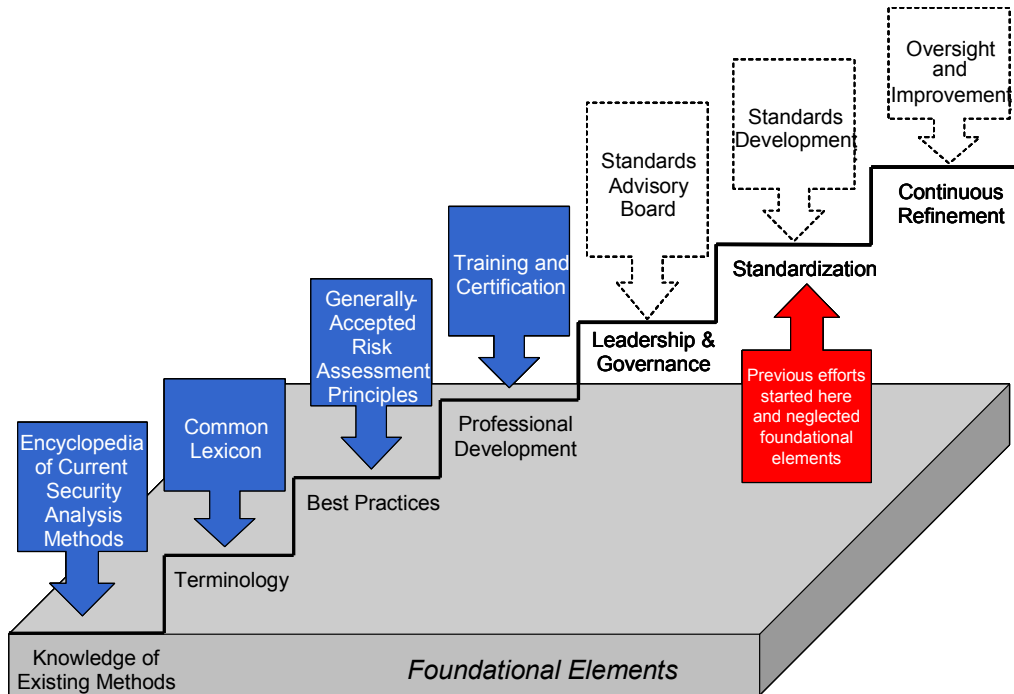


Figure 1. Creating the Foundation of Security Risk Management - The Building Blocks of Success

The underlying reasons for this trend are complex and bear further discussion:

- **Security risk management is an immature discipline that has developed independently and unevenly across the Federal Government and private industry.** DHS leadership correctly seized on the applicability of security risk analysis to the mandate of protecting the homeland, but it failed to ensure the processes and cadre of experienced risk analysts necessary to effectively serve the mission were in place. As such, there is still no system of standardized professional development to attract and educate the number of risk management practitioners the homeland security mission requires.
- **There is no national system of governance available to risk practitioners for collaborating on building interoperability into their risk management approaches.** Lacking an interagency advisory board or recognized standard-setting body, there is no way to synchronize divergent methods, arbitrate disputes or resolve crosscutting issues. Consequently, security risk practitioners often develop new methodologies rather than adopt, or adapt, an existing approach that doesn't fit their needs exactly. Furthermore, because the underlying methods are not based on recognized or compatible metrics,

the resulting data is often useless to other agencies that must then collect similar data using another methodology.

- **There is no comprehensive, documented body of knowledge on the current state of the security risk management discipline.** There is no encyclopedic reference to which practitioners may refer when considering how to best meet their security risk analysis needs. Without this body of knowledge, there is no way to determine where adequate methods already exist, decide where to focus additional research and development or ensure existing efforts are not duplicative and wasteful. Moreover, without this collection of knowledge, it will be difficult to train the next generation of security risk analysts and managers in a consistent manner.
- **The lack of a common professional language for security analysis and risk management divides practitioners and makes collaboration difficult.** This "language deficit" serves as a fundamental impediment to a cooperative approach on security risk analysis by the Government and the private sector. While many attempts to dictate standards within individual Federal departments and agencies have been attempted, their conflict with similar efforts elsewhere only exacerbates the problem. Without a common language to be used by practitioners when describing methods and needed improvements, future progress will remain frustratingly slow.
- **Looking to the future, there is currently no capability to train or certify the knowledge of security risk management professionals.** Given the huge investments being made in homeland security, coupled with the central role of risk management, it would seem logical that training and certification of current and future practitioners is a national requirement. Unfortunately, there is currently no recognized approach to risk management training for practitioners in Federal, state, and local government agencies, or in the private sector. Absent this, it is difficult to imagine that risk management will ever be done with accuracy, reliability or consistency.

## **Discussion**

*"The need for and difficulties associated with creating a coordinated, coherent risk management approach to the nation's homeland security have been widely acknowledged since the events of September 11, 2001, and the creation of DHS. Yet, this general acknowledgment has not been accompanied by the guidance necessary to make consistent use of risk management across DHS."*

U.S. Government Accountability Office  
Applying Risk Management Principles to Guide Federal Investments, GAO-O7-386T

Without the leadership and guidance necessary to overcome the noted challenges to applying security risk management processes and methods in a consistent manner, an intensely competitive environment between Federal departments and agencies, the contractors who support them, the National Labs, and academia has developed. The resulting free-for-all has slowed progress on this issue to a virtual standstill.



As long as each Federal department and agency stands alone, synchronization of methods and the ability to validate the conclusions of the resulting assessments is not possible. The net effect is that, since 2001, over \$12 billion<sup>1</sup> has been distributed to state and local governments by DHS based on assessments of risk that do not provide any means to quantify the overall impact of the funds and that do not meet any recognized standard. Moreover, the almost annual changes to the process for allocating funding has prevented any sort of baseline from emerging and makes it virtually impossible to know if, in fact, the Nation is any safer now than before 2001.

Recognizing the need for a constructive forum to collaborate, improve professional methods and share information in a non-threatening environment, security practitioners have begun to take matters into their own hands. For example, the Security Analysis and Risk Management Association (SARMA) was formed in 2005 to help promote a balanced, cooperative approach to advancing security analysis methods and the profession in general. Likewise, the American Society for Industrial Security (ASIS) has begun developing its own risk management standard to fill the void in Federal security efforts. Even international organizations, such as the Risk Management Institute of Australasia, have stepped in to fill the void with an effort to document a common body of knowledge for security risk management. As such grass-roots movements gain momentum, the Federal government risks slipping still further behind in shaping the future of security risk management.

This problem is not insurmountable, however. In fact, a similar problem has been successfully addressed before. In 1988, then President Ronald Reagan issued National Security Decision Directive (NSDD) 298, which created a National Operations Security (OPSEC) Program in order to coordinate the efforts of all Federal departments and agencies with national security missions. Among other things, NSDD 298 created the Interagency OPSEC Support Staff (IOSS) to help promote sound methods and educate current and future generations in the use of the OPSEC methodology. Concerned practitioners also joined their efforts with those of the IOSS by creating the OPSEC Professionals Society to further the application of OPSEC as a professional discipline and foster high standards of professionalism and competence among practitioners.

## **A Path Forward**

The urgent need for improved security risk management processes and consistent implementation across the Federal government requires strong leadership, a bold vision for coordinated governance, and a comprehensive plan to implement the partnerships necessary for a ***national strategy*** on security risk management. The past two decades have shown that the “every agency for itself” approach will not result in a coordinated national approach, as doing so is beyond the mission and authority of any one Federal department or agency. The Government Accountability Office (GAO) and Congressional Research Service (CRS) have both come to recognize this may be the case. In a December, 2005, report on homeland security risk management, GAO concluded:

---

<sup>1</sup> Congressional Research Service, The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress, Order Code RL33858, Feb. 2, 2007, available at <http://www.fas.org/sgp/crs/homesecc/RL33858.pdf>, accessed Sept.25, 2007

*"For the results of a risk management system to be meaningful and useful, all related agencies should be using similar methods. If agencies' methods are not compatible, then comparisons between agencies become difficult and sector or national risk assessments becomes less reliable."<sup>2</sup>*

CRS went further in detailing the importance not only of an interagency approach, but a National one that necessitates partnerships with those outside of the Federal government:

*"A cohesive risk strategy and agreement on core terms amongst disparate agencies is desirable because many aspects of the risk management process are dependent on functions performed by agencies outside of the department. However, the necessity of common definitions and standards goes beyond the federal government. As states and localities continue to provide information to be included in the risk assessment process, to include, information on critical infrastructure sites within their respective jurisdictions and, eventually, investigative information, the rationale for attempting to develop national-wide risk assessment strategy at all levels of government becomes stronger."<sup>3</sup>*

We end this subsection by proposing a framework for decision makers to consider regarding the governance required to improve risk management nationally. The authors believe the essential elements of such a framework would include:

### **Leadership**

Resolution of the interagency leadership problem requires a clear mandate from the White House to overcome the existing challenges. Steps that should be taken include:

- **Issuing a National Security Presidential Directive (NSPD) or Homeland Security Presidential Directive (HSPD) creating a "National Security Risk Management Program"**. The HSPD/NSPD should establish a national program for security risk management, complete with funding for a system of governance of Federal efforts to produce a government-wide approach. Through such a program, the White House could accelerate progress, reduce massive duplication of efforts, and eliminate organizational conflicts and other barriers.
  
- **Creating a security risk analysis governance infrastructure to help bring rigor and standardization to the assessment of security risks, while increasing confidence in the outcome.** To this end, the creation of the following two organizations is recommended:

---

<sup>2</sup> U.S. Government Accountability Office, Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure, GAO-06-91, Dec. 2005, available at <http://www.gao.gov/new.items/d0691.pdf> accessed Sep. 25, 2007

<sup>3</sup> Congressional Research Service, The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress, Order Code RL33858, Feb. 2, 2007, available at <http://www.fas.org/sgp/crs/homesecc/RL33858.pdf>, accessed Sept. 25, 2007

- ***A Security Advisory and Risk Standards Board (SARSB).*** A SARSB would be officially recognized as the authoritative body for Federal security risk management strategy, policy and standards. Similar in concept to the approach used by the Financial Accounting Standards Board (FASB) in establishing Generally Accepted Accounting Principles (GAAP) for the accounting industry, it would provide oversight, guidance and standards development for all Federal agencies. The leadership of the SARSB should include representatives from all agencies with significant homeland security and national security responsibilities.

The role of the SARSB would be to:

- Develop a national architecture for Federal security risk management and work in partnership with state and local government, the private sector, professional associations and academia to translate the architecture into a roadmap for implementation.
- Be the Government’s authority on security risk management, with responsibility for developing voluntary consensus standards and recognizing best practices.
- Advise all Federal departments and agencies on the development of new risk assessment methodologies, programs and policies, and promote the convergence of existing approaches toward more unified and compatible methods.
- Specify national level requirements for intelligence and counter-intelligence information needed to support the threat analyses to be used in risk assessments.
- Provide an annual report card on the progress of individual Federal agencies in implementing risk management programs to support security decision-making and investment prioritization.
- On an as-needed basis, chair dispute resolution meetings with Federal departments or agencies with disagreements over security risk management activities and policies that may affect national/homeland security interests.

- ***An Interagency Risk Management Support Staff (IRMSS).*** The function of an IRMSS would be to provide program development support, technical expertise and training to Federal, state and local governments, as well as the private sector. Addressing the shortage of qualified risk methodologists and trainers in the Federal Government, the IRMSS mission would centralize that expertise, making it available in one place to support practitioners in achieving the national goal of a mature, unified and broadly-accepted approach. It is also possible that such a mission could be delegated to an existing organization, such as the Interagency OPSEC Support Staff, which has deep experience in supporting the national OPSEC Program at an interagency level.

The role of the IRMSS would be to:

- Support the National Risk Management Program by providing tailored training and assisting in program development.
- Produce educational multimedia products and presenting at conferences for the homeland security, defense, intelligence and public safety communities.
- Help Federal, state and local government organizations develop self-sufficient interoperable risk management programs in order to protect the American public, infrastructure and activities.

### **Guidance**

Through the aforementioned approach, the White House could direct:

- **Federal departments and agencies to create a Chief Risk Officer (CRO) position to synchronize, coordinate and monitor all security risk efforts within their organizations.** The CRO concept has been in widespread use by the private sector for decades. Implementing such a position within key Federal departments and agencies would elevate the importance of risk management and end debates over who creates the necessary policies and procedures and leads the risk management initiatives at the department and/or agency-level.
- **Mandate that Federal departments and agencies participate in resolving their differences through the SARSB.** Participation in a respected, non-governmental body, such as the SARSB, would help to elevate the discussion beyond the unique and sometimes parochial interests of Federal departments and agencies that have often doomed previous attempts to improve the uniformity of risk management methods.

### **Public-Private Partnerships**

Any comprehensive solution must also include active partnerships with the security industry as an integral partner in achieving national plans, such as the National Infrastructure Protection Plan (NIPP). Therefore, the White House should consider recognizing appropriate security analysis/risk management professional associations as partners in representing the private sector, academia and the security risk analysis profession at large. Federal departments and agencies should seek to benefit from the deeper and broader experience available through such associations. The creation of this public-private partnership is necessary to establish communication and buy-in between Federal and private sector practitioners engaged in supporting national and homeland security missions. Such participation will allow for the broadest input and greatly facilitate the adoption of standards by the private sector. In turn, this will lead to a more uniform implementation of security risk management in the United States.

SARMA is one such association working to address many of the necessary foundational elements through its Common Knowledge Base (CKB) Program. The initial focus of CKB Program is threefold: 1) documenting the analytical methods

already in use; 2) establishing a common lexicon for security risk analysis; and, 3) developing standardized approaches to key security risk analysis issues. To that end, three specific projects have thus far been initiated:

- The **Common Lexicon Project** is focusing on developing a broad-based, consensus solution to the "language barrier" through the orderly collection of existing terms, linguistic deconstruction of definitions, and the application of a consensus process to arrive at acceptable common definitions.
- The **Encyclopedia of Security Analysis and Risk Assessment Methods** is using a Wiki-based approach to allow security practitioners across the nation to provide documented descriptions of their methodologies in a current "state of the profession" virtual encyclopedia.
- The **Generally Accepted Risk Assessment Principles Project**, or GARAP, is identifying and promulgating common practices and generally accepted principles to bring added rigor and standardization to the process of assessing security risks.

Each of these projects is being implemented in an open and transparent manner to encourage participation by the broadest possible range of security risk analysis practitioners. To learn more, visit the SARMA CKB Program web site at: <http://sarma-wiki.org>.

## **Conclusions**

The terrorist attacks of September 11, 2001, highlighted the difficulty of protecting an almost infinite number of targets with finite resources. The use of security risk management is the approach chosen by our Nation's leadership to address this problem. Yet, in order to ensure the effectiveness of this effort and accurately quantify its impact, the development and implementation of a national strategy for security risk management is needed. The refinement and application of a more uniform and coordinated approach to analyzing security risks will greatly enhance our Nation's ability to understand and manage a multitude of risks. It will also lead to improved decision-making by Congress and the White House, as well as more efficient prioritization of resources.

The creation of such a national system of governance and standards for security risk management is beyond the mission and authorities of any one Federal department or agency. Even with visionary leadership and direction it will not be easy, as the U.S. Government Accountability Office and others have noted. Yet such a system is necessary if we are to protect the people, infrastructure and economic prosperity of the United States. The authors encourage the White House, Congress, Federal departments and agencies, State and local governments and the security profession to join forces and strive to achieve a National security risk management program that will help provide the Nation the security it needs at a price it can afford.

## About the Authors

### *Edward J. Jopeck*

Ed Jopeck is a Senior Principal at SRA International specializing in security analysis, risk assessment, risk management, intelligence and infrastructure protection. Over his 20-year career in the field he has developed, evaluated and applied security risk assessment methodologies in the intelligence, defence and homeland security communities. Between 2003 and 2007 he served as a security risk management consultant to the US Department of Homeland Security, where he led the development of strategic-level antiterrorism risk analysis methods and initiatives. He has also led antiterrorism risk assessments of large U.S. water supply systems serving nearly 12 million people, and assessed 19 federally-owned high-hazard dams, and associated hydropower plants.

Prior to September 11, 2001, Mr. Jopeck worked as an intelligence and security analyst for the Central Intelligence Agency, and later as a security analysis and risk management consultant to numerous other governmental organizations. While at CIA, Mr. Jopeck was a key developer and lead instructor of the CIA's Analytical Risk Management training program which was awarded a National Intelligence Meritorious Unit Citation by the Director of Central Intelligence.

Mr Jopeck is currently serving his second term as the Founding President and Chairman of the Board of the Security Analysis and Risk Management Association (SARMA), a professional association working to mature security risk management practices and advance the profession of security analysis.

### *Kerry L. Thomas*

Kerry Thomas recently joined the Washington Federal Practice (WFP) of PricewaterhouseCoopers (PwC) after more than ten years of Federal service. Mr. Thomas is currently overseeing the development of PWC's enterprise risk management solution for government agencies, as well as working to develop a suite of grant-related services for Federal clients. His work also includes advising various government and private sector clients on homeland security, risk management and grant-related matters.

Mr. Thomas previously served as a senior official within the U.S. Department of Homeland Security where he was responsible for the development of policy, as well as oversight and management of a broad range of grants, technical assistance programs, risk assessments and other services for the protection of critical infrastructure and key resources.

Mr. Thomas is also currently serving as the Executive Vice President of the Security Analysis and Risk Management Association (SARMA), and as a member of the SARMA Board of Directors. He has a Masters Degree in Public Management from the University of Maryland in College Park, Maryland, and a Bachelors Degree in Political Science from Texas Christian University in Fort Worth, Texas. A native of Texas, Mr. Thomas has resided in the Washington, D.C. area since 1993.



**Profitability and Environmental Reliability:  
Risk, Resources and the U.S. Petroleum Industry**

Frederick Wolf, DBA  
School of Business  
Pacific Lutheran University  
Tacoma, Washington, 98447-0003  
wolffg@plu.edu

**Abstract**



This paper will examine the link between corporate profitability, economic sustainability and the environmental reliability of the petroleum industry in the United States. This is an empirical study based on ten years of data (1996-2006). The investigation builds upon the earlier work of Rose (1990) involving airline safety. Rose determined “richer was safer” when it came to airlines; but this important research stream has not been extended to other classes of industry or organizations. The nature of profitability in this sector will be examined. Its impact on environmental reliability will be made explicit, and the nexus of profitability and environmental reliability to organizational sustainability will be explored and further developed. The link between profitability and reliability is contingent on managerial choices involving resource allocation for the purpose of repair and maintenance, equipment upgrading and acquisition of new technologies. We will argue for a more comprehensive and robust approach to discretionary spending that has the potential to improve not only the environmental reliability of the petroleum industry, but also the industry’s sustainability in a very dynamic socioeconomic setting.

### **Introduction**

This paper extends previous research into the role of resource availability on the reliability and safety of organizations as complex technical systems. According to the resource based view (RBV) the firm’s resources are bundled to enable the firm to achieve above average returns. Resources enable a firm to execute strategy to out perform its completion or to reduce its own vulnerabilities. This paper deals explicitly with resources and is not focused on capabilities. The study described in this paper examines the relationships between resource availability and resource utilization or commitment on the environmental reliability of the firm.

Consistent with the previous literature (Feinstein, 1989) (Moses and Savage, 1989) (Rose, 1990) (Marcus and Nichols, 1996), (Marcus and Nichols, 1999) that provides the theoretical basis for this work, the focus of this study is at the level of the firm and not on specific production processes such as manufacturing plants and facilities.

The focus of the paper is on resources and reliability. Reliability is fundamental to understanding and achieving safety through a process of risk reduction involving all classes of technical systems; it is the ability of the system to maintain its function in routine and non-routine circumstances either anticipated or unanticipated. Environmental reliability is the ability of an organization to meet its environmental health and safety risk management objectives and obligations under various circumstances and conditions.

### **Literature and Theoretical Framework**

Any discussion of the role of resource availability on system performance at the level of a firm must address the construct of reliability. While organizational scholars debate the subjective nature of safety and risk as enactments of perception, this paper will take a more objectivist perspective by drawing upon the engineering view of reliability which is grounded empirically in the behavior of technical systems. As minor, untoward incidents increase in frequency, the risk of a major untoward incidents having more dire consequences increases as well. Therefore, if the number of untoward events having minor consequences can be reduced, the risk of a more sever event will also be reduced. This model of risk can be stated as:

$$\text{Risk} = (\text{Probability of some untoward event}) (\text{The consequence of the event})$$

According to this model, the likelihood of an event is some function of the probability of lesser events which can be identified and controlled. While we can not observe safety or reliability directly, we can observe incidents and accidents which provide insight into the underlying probability density function that describes the risk. Because the risk is defined in terms of a probability of an event times its consequence, an organization can intervene to reduce the risk of an outcome by reducing its probability. This is the basis for all modern safety programs; safety is measured in terms of the rate of some pertinent minor event. As incident frequency is reduced, the likelihood of a more significant untoward event (and its outcome) is also reduced. Therefore, safety and risk are both outcomes related to system reliability.

Osborn and Jackson (1988) investigated the role of resource intensity (investment in nuclear technology) and earnings growth on reliability for a sample of 26 utilities operating 41 separate nuclear powers plants. They found higher capital investment (or intensity) in nuclear power technology linked to a lower rate of minor incidents. The link between earning growth and reliability was not significant. Surprisingly, they discovered for those utilities with less capital investment in nuclear technology, the number of minor incidents decreased with increased profit growth (as would be expected) but, for utilities with greater capital intensity in nuclear technology, the number of major incidents increased with earnings growth. Osborn and Jackson interpreted this as an indication that: ...characterized highly committed utilities as cautious when less-profitable and embarking on bold calculated risks when flush. Their characterization is consistent with our description of a riverboat gambler (1988, 942).

Rose (1990) studied the role of resource availability on the safety of airlines operating in the United States during the period 1981-86. In this work, the determinants

of airline safety were considered as two orthogonal constructs: safety investment (as resource commitment) and operating conditions (associated with environmental and climatological conditions) associated with the route of flights used by the specific airline. Rose argued: “Air carriers chose their level of safety investment by balancing the cost of additional safety-enhancing investments with the benefits of reducing accident or incident risk” (1990, 946). In this study, airline resources were measured using operating margins (as a measure of operating profitability), interest coverage (a measure of financial leverage), working capital and current ratio (both of which address liquidity issues). Airline accidents were a surrogate measure of reliability and the study attempted to control for the effects of weather en route by incorporating a dummy variable for flights operating into and out of Alaska, the total number of miles flown,, operating experience with the aircraft type and the total number of departures.

Airline accidents were rare and found to follow a Poisson probability distribution, as would be expected. A basic Poisson regression model was used to test the data. Rose concluded airline profitability is directly correlated with airline safety (as determined by accident rates). Higher operating margins were associated with reduced accident rates.

Rose further states:

The empirical findings are consistent with models in which corporate investment, including investment in product safety, is affected by financing constraints, limited liability, and reputation formation. Although the present data are not strong enough to distinguish among these competing explanations, additional power might be gained from direct analysis of safety investment and other measures of airline quality. If the casual relationship between financial conditions and safety levels is casual, we would expect to observe similar financial effects on both safety investment levels and other aspects of airline quality. The results presented in this paper argue strongly for further empirical research along these lines (1990, 960).

Following in the path of Rose (1990), Marcus and Nichols (1996, 1999) investigated the relationship between resource availability and resource commitment on the reliability and safety of nuclear power generated by public utilities. They used Significant Events (SE) as an indicator of system reliability. Significant Events (SEs) are a nuclear industry specific variable that includes several related outcomes including an unexpected plant response, the degradation of important safety equipment, complicated shutdowns and unplanned radioactivity releases. Marcus and Nichols operationalized resource availability as the financial ratio Return on Assets (ROA) and the debt to equity ratio, D/E. They considered resource commitment as the ratio of plant cost per megawatt capacity and two separate variable cost components, 1) operations, and supervision expense per megawatt capacity and 2) maintenance supervision and maintenance expense per megawatt capacity. They attempted to control for differences in generating strategy and regulation. They found resource availability (as ROA) had no statistically significant effect of significant events, but commitment of resources did. Interestingly, they also found regulatory scrutiny was significantly related to significant events (Marcus and Nichols, 1996, 1999) This finding suggests a reactive enforcement posture on the part of the regulatory community where a history of SE's trigger more inspections.

Russo and Fouts (1997) found support ( $p < .004$ ) for their hypothesized relationship that high levels of environmental performance are associated with enhanced profitability among a sample of 477 firms that spanned all industrial sectors. They also found: "...higher environmental performance is associated with higher financial

performance and this relationship is strengthened as industrial growth rises.” (1997, 549)  
Although the effect was modest.

Bowen (2002) suggests organizational slack and visibility impact environmental performance in predictable ways. Specifically, Bowen concludes a firm’s size is not predictive of environmental responsiveness, rather resource availability as slack does. This observation is consistent with Perrow’s Normal Accident Theory (1999) whose core hypothesis suggests system level risk is some function of interactive complexity and coupling. Coupling according to this theory is a variable that includes among other constructs, resource availability conceptualized as slack resources.

McGuire, Sundgren and Schneeweis (1988) found ROA had a predictive association with Fortune magazines’ rating of corporate social responsibility. Among other characteristics that are used to score corporate social responsibility were financial soundness, long-term investment value, use of corporate assets, quality of management, innovativeness, quality of products of services, use of corporate talent, and community & environmental responsibility. The strength of the relationship during the period 1971 to 1984 was strong ( $R^2 > 0.5$ ) and significant ( $p < .01$ ). Strong ROA performance within a sector should reflect differences, among other things, in the effectiveness of management.

### **Hypotheses**

This study investigates three hypotheses related to resource availability and commitment related to firms in the same sector, petroleum refining.

The first hypothesis addresses changes in resource availability and reliability. Firms in the same industry should enjoy greater reliability (and present lower risk) with

greater resource availability. As resource availability increases, reliability should improve.

*Hypothesis 1* Firms from within the same sector that have greater resource availability should have greater reliability.

The second hypothesis considers resource commitment. Firms within the same sector that commit more resources to process and production improvement, should exhibit greater levels of system reliability.

*Hypothesis 2* The reliability of firms within the same sector that commitment more resources to system improvement through greater capital spending per unit of production should be more reliable than other firms.

The third hypothesis addresses capacity utilization. As capacity utilization increases, asset turnover increases, which in turn, improves return on asset performance. Therefore, as financial performance improves, resources should become less scarce and reliability should increase.

*Hypothesis 3.* The reliability of firms with in the same sector should improve with higher rates of capacity utilization.

## **Methodology**

### *Sample of Firms*

Eleven (11) firms were included in the sample. Firms were chosen from those within the petroleum refining sector for which financial information could be obtained. During the time frame of the study (1996-2006) considerable consolidation and change occurred in this industrial sector. In 1996, there were 91 firms operating in the petroleum refining sector in the United States. By 2007, there were 51. (Leffler, 2007) Information

on the financial condition of the 11 firms in the sample was obtained from publicly available sources.

### *Measures*

This investigation examines the rate of accidental hazardous substances releases (incidents) per unit of production. In this case the unit of production is 10,000,000 barrels of crude oil processed. One barrel of crude oil represents about 42 gallons of raw material feed stock. From this volume, roughly 62 gallons of various hydrocarbon products are generated. Accidental hazardous chemical releases are a measure of reliability that relates directly to environmental risk. Other measures include resource availability as Return on Asset (ROA) performance and Resource Commitment as Capital Spending per barrel of production.

### Dependent Variable

Accidental hazardous chemical releases occur when such substances are instantly released to the environment in unanticipated and unplanned ways. These events can range in significance from trivial spills of slightly over 1 pound of marginally hazardous substance to huge accidents involving the accidental release of over 10,000 pounds of an extremely toxic gas such as hydrogen sulfide. All such events must be immediately reported to the National Response Center (NRC). Each record of a report is maintained in the Emergency Response System Notification (ERNS) data base which can be publicly accessed via the NRC website.



Accidental hazardous substance releases are incidents which can be used to understand and measure the environmental reliability of this class of industrial firms. The number of such events and their frequency is directly associated with the risk of such firms. By definition, risk is the product of the likelihood of an event times its consequence. As the frequency of small, untoward events increases, reliability theory warns the probability of a more serious, potentially catastrophic event, also increases.

These events can occur anywhere in the value chain of the firms in the sample. They can occur during production, manufacturing, storage, transportation and distribution. As such, they represent a system level measure of environmental reliability and risk. The rate of accidental hazardous chemical releases per 10,000,000 barrels of crude oil processed was calculated by year (1996-2006) for each firm in the sample.

#### Independent Variable-Resource Availability

Resource availability is measured by Return on Asset (ROA) for each corporation calculated for each year in the study period (1996-2006). Return on Assets (ROA) is the product of two key variables; profit margin and asset turnover. Petroleum products are commodity-like; typically characterized by low profit margins and moderate demands that produce sufficient asset turnover to allow for a reasonable return on assets. This measure is a viable surrogate of resource availability that links back to earlier work by Marcus and Nichols (1996, 1999) and to Rose (1990) where profit margin, an important component of ROA, was considered.

### Independent Variable-Capacity Utilization

Capacity utilization, expressed as a ratio of actual production to rated capacity is a measure of asset turnover. It is an indication of market demand as well as production efficiency. As such, it is an important determinant of economic success.

### Independent Variable-Resource Commitment

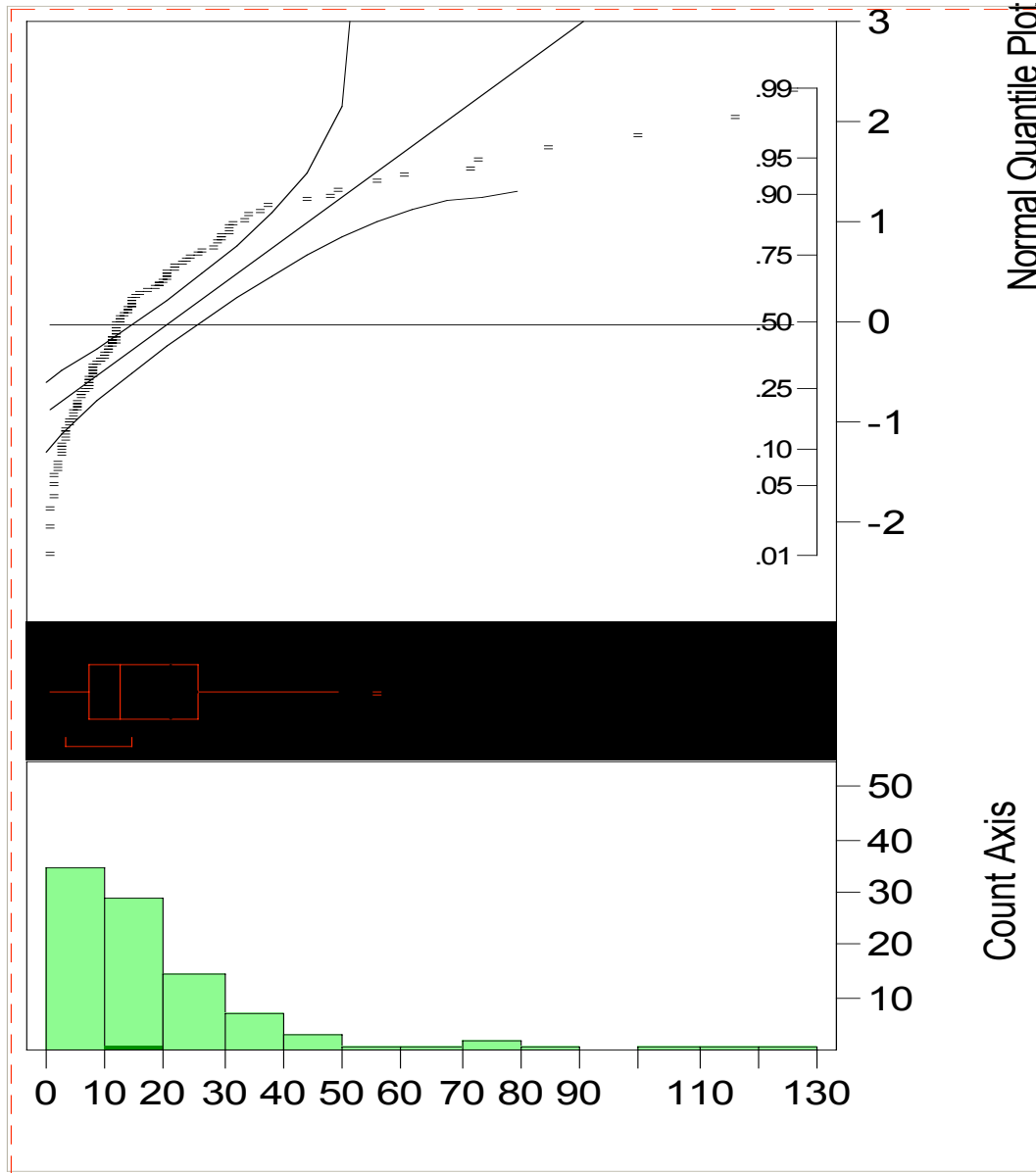
Resource Commitment is measured as the ratio of Capital Spending per unit of production calculated for each year in the study period (1996-2006). Capital spending is a direct measure of the capital investment in the business. It reflects the amount of resources committed to upgrading, improving and enlarging productive capacity within the firm. Petroleum refining is a capital intensive industrial sector. Because the amount of capital spending varies widely according to the size of the firm, the amount of capital spending must be normalized to the production throughput to enable meaningful inter-firm comparability.

### *Analysis*

Figure 1 illustrates the distribution of the dependent variable, the rate of accidental hazardous substance releases per 10,000,000 barrels processed, during the ten year study time frame. Clearly, this variable is truncated and left censored. Consistent with previous research in the field of accident and incident rates, statistical analysis was performed using Poisson regression. The Poisson has been recognized as the appropriate latent model for rare events such as accidents and similar incidents and their rates. These are rare events and their distributions are left centered, conditions which violate the

assumptions that support the use of Ordinary Least Squares regression for hypothesis testing.

**Figure 1 Distribution of Accidental Chemical Releases per Unit of Production**



## Results

Descriptive statistics and Pearson product moment coefficients for all data used in this study are presented in Table 1.

**Table 1 Descriptive Statistics and Pearson Product Moment Coefficients**

Parameter	n	mean	standard deviation	X1	X2	X3	X4
Releases/unit of production	111	20.699	23.516	1			
ROA	111	0.074	0.159	-0.211*	1		
Capital Spending/unit of production	111	56.659	36.164	0.212*	0.222*	1	
Capacity Utilization	111	98.265	1.288	-0.353*	0.154	0.015	1

\* $p < .05$ ; \*\* $p < .01$

Because there is evidence of correlation between ROA and Capital Spending/unit of production, the relationship between these variables was examined using Ordinary Least Squares Regression (OLS). Return on Assets was treated as the independent variable and Capital Spending/Unit of Production was the outcome variable. The  $R^2$  of the model was 0.049 and was significant ( $p < .03$ ). The effect was small though it was significant. To test the hypotheses considered in this study, five Regression Models were created. All models used the rate of accidental hazardous chemical releases per unit of production as the outcome variable. The first model included ROA for each of the firms for the ten years associated with the study. The second model included Capital Spending per unit of production for each of the firms during the ten years associated with the study. Model three included both ROA and Capital Spending per unit of production for each firm during the ten year time frame of the study. Model 4 examined capacity utilization alone. Finally, Model 5 included ROA, Capital Spending, and Capacity Utilization. The data was modeled and tested using SHAZAM Version 9.0 in the maximum likelihood

estimation (EPOISSON) mode. This model is appropriate when the outcome variable is count data or ratios as was the case in this investigation. (Northwest Econometrics, 2001)

The results of the modeling exercise are presented in Table 2.

**Table 2 Poisson Regression Models: Coefficients, Significance and Fit**

Variable or Statistic	Model 1	Model 2	Model 3	Model 4	Model 5
ROA	-2.6933**		-31.430**		-2.4181**
Capital Spending/Unit of Production		0.0093**	0.0325**		0.0012**
Capacity Utilization				-0.1589**	-0.1368**
Poisson $R^2_{(p)}$	0.0961	0.0089	0.1094	0.0815	0.1597
Poisson $R^2_{(d)}$	0.0732	0.0046	0.0809	0.0438	0.1116
$G^2$	2034.9	2185.6	2018.0	2099.3	1950.8
Log of Likelihood Function	-1259.11	-1334.45	-1250.67	-1291.37	-1217.03

\* $p < .05$ ; \*\* $p < .01$

Table 2 contains the results of the modeling including the coefficients for the independent variables, statistical significance, and measures of fit including  $R^2_{(p)}$  which is derived from the standardized residuals,  $R^2_{(d)}$  which is likelihood ratio index and  $G^2$ , the sum of the deviances. The most widely used measure of goodness of fit for Poisson models is the  $G^2$ . In the interpretation of Poisson regression models, the smaller the value of  $G^2$ , the better the fit. (Greene, 2000)

Model 1 relates accidental chemical releases per unit of production to return on asset (ROA) performance. The coefficient of ROA is significant ( $p < .01$ ) and the sign of the coefficient is directionally consistent with Hypothesis 1. Model 2 relates accidental chemical releases per unit of production to resource commitment as determined by capital spending per unit of production. Again, the coefficient of Capital Spending per unit of production is significant however its sign is not directionally consistent with Hypothesis 2. The  $G^2$  of Model 2 shows no improvement over Model 1 (2034.9 vs.2185.6) and the

difference in the Log of the Likelihood functions between Model 2 and Model 1 indicates Model 1 is significantly ( $p < .01$ ) more powerful. When ROA and Capital Spending per unit of production are included in Model 3, both coefficients are significant ( $p < .01$ ) but only ROA is directionally consistent with the expectation of fewer accidental hazardous chemical releases. Model 3 shows significant ( $p < .01$ ) improvement over Models 1 and 2 based on its  $G^2$  (2018.0) and the log of its Likelihood Function (-1250.67) suggests significant ( $p < .05$ ) improvement over Model 1. This finding suggests both resource availability (as ROA) and capital spending per unit of production are significant factors influencing the environmental reliability of this class of firms. Although the directionality of the effect associated with capital spending is surprising. Model 4 simply investigates the effect of capacity utilization by itself. Its effect was statistically significant ( $p < .01$ ) in the model. Model 5 includes all three effects, ROA, Capital Spending per unit of production and capacity utilization. The final model yields the lowest value of the  $G^2$  parameter which indicates the best fit among the other models and its log of the Likelihood function is significant ( $p < .01$ ) when compared to the other models.

Because the outcome variable was overdispersed, which is a special case of the Poisson distribution, further modeling was performed using negative binomial regression (NEGBIN model in SHAZAM Version 9.0). The results of the Negative Binomial Regression modeling are presented in Table 3. The results of modeling the effects associated with ROA, Capital Spending per unit of production and Capacity Utilization using Negative Binomial Regression closely follow the Poisson modeling outcomes. Again, Model 5 which included the three effects, yielded statistically significant ( $p < .01$ )

coefficients for all three effects; although small, the highest value of  $R^2$  and a significant ( $p < .01$ ) Log of the Likelihood function compared to Models 1 & 3.

**Table 3 Negative Binomial Regression Models: Coefficients, Significance and Fit**

Variable or Statistic	Model 1	Model 2	Model 3	Model 4	Model 5
ROA	-29.2401**		-31.4321**		-27.9140**
Capital Spending/Unit of Production		0.0061*	0.0325**		0.0033**
Capacity Utilization				-3.2258**	-2.9940**
$R^2$	0.0383	0.0079	0.0452	0.0324	0.0705
Log of Likelihood Function	-2643.3	-2645.5	-2642.9	-2643.97	-2338.22

\* $p < .05$ ; \*\* $p < .01$

### Discussion

This investigation provides support to the notion that resource availability as suggested by Return on Assets is negatively related to accidental hazardous substance releases. The greater the ROA, the lower the rate of accidental releases in the sample of 11 petroleum refining firms during the 10 year period, 1996 to 2006. This finding is entirely consistent with Rose (1990) and our expectations. In the field of finance, ROA is considered a basic measure of the efficiency with which an organization allocates and manages resources. If a corporation desires to improve its ROA, it must increase its profit margin and/or its asset turnover. In the petroleum refining business, which is commodity-like and dominated by economies of scale, profit margins typically are less than 10% with asset turnovers typically equal to or greater than 1.

That ROA is inversely related to accidental chemical releases per unit of production suggests those firms who are more effective at generating profit and turning over assets are measurably and significantly more reliable and hence safer. Interestingly,

this finding also suggests a paradox that could occur as the result of management initiatives to improve ROA through rapid inventory turnover (such as Just-In-Time Inventory Control) which have the potential to simultaneously improve reliability by generating more resource availability as suggested by increased ROA while making the system more tightly coupled, which according to Normal Accident Theory would make the organization more prone to catastrophic outcomes. (Perrow, 1999)

Profit Margin, the other component of ROA, is determined through pricing strategy and through the control of operating costs. Given the fact that hydrocarbon fuels are commodity-like products, manufacturing scale dictates pricing; which is to say, the largest producer can set price. All other firms in the sector must rely on effective management of operating costs to achieve a favorable profit margin. Perhaps the improvement of profit margin through organizational initiatives including Total Quality Management (TQM), Continuous Process Improvement, Six Sigma, and the implementation of comprehensive Process Safety Management programs underway since the mid-1990's has resulted in improved ROA through increased reliability.

To see if there is a trend in the rate of accidental hazardous chemical releases per unit of production, the mean rate for the first five year period (1996-2000) was calculated. During this period, the mean rate was 23.75 releases per 10,000,000 barrels processed. The mean rate during the subsequent five year period (2001-2006) was 22.12 releases per 10,000,000 barrels processed. This difference is significant ( $p < .05$ ). During the same periods, the mean ROA for the firms in the sample increased from 2.76% to 11.76%. This finding is particularly interesting as it also reflects the period preceding and immediately following the change in political control of the executive branch of the



United States from the Democrat Clinton to the Republican Bush administrations. This period is believed by many to represent a change in national environmental policy from a more environmentally concerned federal government to one that is less committed to environmental outcomes. As for environmental reliability, as determined by accidental hazardous chemical releases, there was no detrimental effect observed in the sample of petroleum firms. While ROA increased so did the environmental reliability (the improvement was small but significant) of the 11 firms represented in this sample.

This research addresses a small, but never the less, significant factor in understanding the nature of risk associated with the petroleum processing sector. Profit margin has a small, but significant role as a factor in determining ROA as well as environmental reliability. This is an important realization because it has some interesting ramifications. Many, including Perrow (2007) have argued "...this is a wealthy highly profitable industry. We should expect more of it (regarding its environmental reliability)..." Perrow argues its size is problematic, that big corporations are necessarily riskier than smaller ones. (2007) His assertions are not necessarily supported by these findings. The largest firms did not experience greater rates of accidental releases per unit of production. In some cases, they experienced fewer net releases than several of the smaller firms. Indeed, some of the smaller firms experienced excellent environmental reliability, but such results did not follow the size of the corporation. Nor did Return on Asset (ROA) performance follow the size of the firm. However, it is the case that commodity economics is closely related to economies of scale, and, *ceteris paribus*, larger manufacturing facilities are generally more efficient. As to whether this sector could be described as "wealthy", the Return on Asset performance demonstrated by the 11 firms

represented in the sample lags many other sectors during the same time period. While the term “wealthy” is entirely subjective, those who share Perrow’s perspective can take comfort in the fact that wealthier is safer at least in this sample.

Additional work is warranted to further identify and develop the theoretical linkage between finance and environmental reliability. More work is needed to fully appreciate how environmental reliability is enacted as a consequence of resource availability. Does organizational slack result in programmatic initiatives that enhance reliability? Certainly, corporate decisions do use ROA as a guide and include the acquisition of new technology, research and development, and production capacity increases. The issue is made more perverse by the fact that growing financial losses can lead to greater risk taking by decision makers. Shapira (1995) This suggests reliability can be tacitly sacrificed for short term financial improvements in underperforming organizations. Such decisions could impact environmental reliability directly and indirectly.

There is evidence that corporate decisions concerning resources have compromised safety and reliability. According to Snow (2007):

Cost cutting efforts created a culture at BP America, Inc. that lead to compromises of system integrity at its Alaska North-slope oil-gathering pipelines and workplace safety at its Texas City, Texas refineries...Virtually all of the seven root causes identified for the Prudhoe Bay incident have strong echoes in Texas City said U.S. Chemical Safety Board Chairwoman Carolyn W. Merritt ...Both reports point to significant budget and production pressures in driving BP’s decision-making-and ultimately harming safety...Both investigations found deficiencies in how BP managed safety of process changes...Other common findings include flawed communication of lessons learned, excessive decentralization of safety functions and high management turnover...One of the primary finding in the (Chemical Hazard Safety Board’s) report was that cost cutting and budget pressures from BP group executive managers impaired process safety at Texas City...and...BP field managers were under extreme pressure to cut costs in Alaska (2007, 30).

The combination of these factors are attributed to be the underlying causes of a series of accidental hazardous substance releases in BP facilities located in the United States. BP America, Inc. was included in the sample of 11 firms represented in this study. During the period 1996-2006, it averaged significantly fewer accidental releases of hazardous substance per 10,000,000 barrels processed than the average of 22.63 for the other 10 firms in the sample. However, its average return on asset (ROA) performance was less than the average of 7.89% for the other 10 firms during the period 1996-2006.

The effect of capital spending per unit of production on the rate of accidental releases of hazardous chemicals was unexpected. The directionality of this relationship suggests increased capital spending is associated with decreased environmental reliability. This contradictory finding is difficult to explain and it is counter intuitive. The literature suggests increased capital spending is a reactive outcome, which in certain cases could explain why increased spending was associated with higher rates of accidental releases. The capital spending associated with such organizations could be an attempt to improve operations, reliability and margins. However there may another explanation for this phenomena documented in the literature of organizations.

Sterman (2000) modeled the effect of cost cutting associated with reduced preventative maintenance in the chemical sector. During the recession of 1974, the chemical industry faced the economic dilemma of increased operating costs coupled with intense pressure to hold down the pricing of its commodity products and Sterman (2000, 70) notes: "Under intense financial pressure, all plants and functions had to cut costs" As preventative maintenance is reduced (as a cost cutting-measure) savings accrue for a short period until uncorrected equipment defects increase the breakdown rate reducing

the on-stream performance of the plant. Based on the ten years of data collected for this study, a significant ( $p < .01$ ) negative relationship exists between capacity utilization and the rate of accidental hazardous chemical releases per unit of production. As on-stream utilization decreases, the rate of accidental releases increases significantly.

When preventative maintenance is reduced as a cost cutting measure, reactive maintenance increases. Sterman observes:

A higher breakdown rate increases costs (due to overtime, the nonroutine and often hazardous nature of outages, the need to expedite parts procurement, collateral damage, etc.) The resulting pressure to cut costs leads to a reduction in the quality of parts, increasing equipment defects and leading to still more breakdowns and still higher costs. Cost pressure also reduces investment in equipment upgrades and other design improvements, so breakdowns increase further (2000, 70-71).

Carried to its conclusion, such cost cutting will lead to the failure of manufacturing systems that will ultimately require replacement. Such replacement costs would lag the initial cost cutting measures by some period of time. The effect could be increased capital spending to replace the production equipment prematurely debilitated and worn out as the consequence of cost pressure and ill-advised attempts to find savings in operational budgets. Consistent with the observation of the positive relationship between capital spending per unit of production and the rate of accidental hazardous chemical releases per unit of production, as equipment wears out and breakdowns more incidents, accidents and other untoward events will occur, perhaps to a peak in frequency and magnitude until the organization decides to take action by making capital investment in the replacement of the failing or failed technology. Thus, it would seem reasonable that increased capital spending in such circumstances would be accompanied by an elevated incident rate including hazardous chemical release accidents. Marcus and Nichols shared this

perspective and elaborated upon it terms of how organizations use accidents and incidents as signals of impending risk for the purpose of resource allocation. They note:

Organizations operate in a broad spectrum of acceptable performance that includes many factors. The problems they face typically arise from the fact that they must respond to constraining requirements, for example the need to be safe as represented by regulators and a need to make money as represented by share holders. A safety boarder may be seen as a set of boundary conditions around economics, work effort and safety which organizations are drawn to overlapping by a desire to optimize on the other dimensions. The feedback they receive as they approach a safety boarder may be weaker and more ambiguous than the feedback they receive when they approach other boundaries such as economics (1999, 484).

Of course, riverboat gambling behavior aside, warning signals must be recognized and heeded to keep the organization from harm. Heeding warning signals may require the commitment of resources to prevent undesirable consequences. When resources are available, management must recognize the warning signal and decide on an appropriate course of action with the appropriate commitment of resources. When resources are not available, there are fewer options available to the organization. Under conditions of resource scarcity, a higher rate of incidents including the accidental releases of hazardous chemicals becomes inevitable.

At this point, the economic viability of the firm becomes threatened as the consequence of lost production and the unreliability of its technology. The sustainability of the firm is degraded and the risk of organizational failure increases. An example of this type of failure is Tosco Corporation, whose cash strapped refineries were plagued by accidents and incidents during the period 1995-97 culminating in a catastrophic accident at one refinery that killed 1 and injured 46. (Wolf, 2001) Tosco ceased to exist after it was acquired by Phillips who later merged to become Conoco-Phillips; its extinction was the

only possible outcome given its profit margins and poor growth potential as it relates to asset turnover.

## **Conclusions**

The conclusions of this study include the realization that environmental reliability as determined by the rate of accidental hazardous substances releases for the sample of eleven firms was significantly (though modestly) related to return on asset performance. This finding is entirely consistent with previous studies, including Rose (1990) that suggests a link between safety (as reliability) and financial performance, specifically ROA.

The observation that capital spending per unit of production was negatively associated with environmental reliability was a surprise. Although, it is possible to posit a plausible explanation as to why this is the case, further research into the underlying salience of this observation is warranted.

The nexus between organizational sustainability and environmental reliability is suggested by return on asset performance. When ROA is less than the sector average, the long term viability of all but the largest firms operating in a commodity market are threatened. Recent research in the field of managerial risk taking suggests as ROA decreases, managers are more willing to forego long term benefits, such as improved reliability in exchange for short term organizational survival. Under such conditions, environmental risks, along with other externalized sources of risk, appear to increase and

managerial decision making becomes more contingent and survival focused. Under these conditions, short term goals become dominant and long term reliability is discounted.

For improved environmental reliability, resources are required. Return on asset performance is an important barometer of resource availability. As such, it can serve as a warning indicator that some organizations (and their managers) may be approaching what has been described as a border of safety. As the reliability of the system decreases, management should be prepared to heed the warning provided by an increased frequency of incidents, accidents and untoward events.

To fail to do so is to gamble with the firm. There are limits to the sustainability of any enterprise. In time, growth will cease and decline will ensue. During the late stages of maturity and decline, resources may become increasingly scarce. When an organization reaches this stage, management should not socialize the cost of reliability by transfer such costs to the public through increased rates of accidental hazardous chemicals; releases to the environment. The commons can not be expected to subsidize, through degradation and the public by exposure to excess risk, the existence of any firm that is no longer capable of sales growth or profitability.

## References

- Bowen, F. (2002) "Does Size Matter?" *Business & Society*, Vol. 41, No. 1 pp. 118-124
- Feinstein, J. (1989) "The Safety Regulation of U.S. Nuclear Power Plants: Violations, Inspections and Abnormal Occurrences" *Journal of Political Economics*. Vol. 97. No. 1 pp. 115-154.
- Greene, W.(2000) Econometric Analysis. (4<sup>th</sup> edition), Prentice Hall. Saddle River, N.J.
- Leffler, W.(2007) "Downstream Mergers, Capacity Hikes Persist". *Oil & Gas Journal*. Vol. 105, No. 24 pp.22-24.
- Marcus, A.. and M. Nichols (1996) "Acquiring and Using Knowledge in Response to Unusual Events in a Hazardous Industry" Presented at the Academy of Management Meeting, Cincinnati, Ohio.
- Marcus, A. and M. Nichols (1999) "On the Edge: Heeding Warnings of Unusual Events", *Organization Science*. Vol. 10, No. 1, pp. 482-499.
- Moses, L. and I. Savage, (1989) Transportation Safety in an Age of Deregulation. Oxford University. New York.
- Northwest Econometrics, (2001) SHAZAM Users Reference Manual. Vancouver, Canada.
- Osborn, R. and D. Jackson (1988) "Leaders, Riverboat Gamblers or Purposeful, Unintended Consequences in Management of Complex, Dangerous Technologies" *Academy of Management Journal*. Vol. 31, No. 4. pp. 924-947.
- Perrow, C. (1999) Normal Accidents. (2<sup>nd</sup> edition), Princeton University, Princeton, N.J.
- Perrow, C. (2007) The Next Catastrophe. Princeton University, Princeton, N.J.
- Rose, N. (1990) "Profitability and Product Quality: Economic Determinants of Airline Safety Performance" *Journal of Political Economy* Vol. 98, No. 5 pp. 944-961.
- Russo, M. and P. Fouts (1997) "A Resource Based Perspective on Corporate Environmental Performance and Profitability" *Academy of Management Journal* Vol 40, No. 3. pp. 534-559.



Shapira, Z. (1995) Risk Taking: A Managerial Perspective. Russell Sage Foundation. New York.

Snow, N. (2007) “U.S. House Cite Similar Problems with BP Line, Refinery”. *Oil & Gas Journal* Vol 105, No. 24 pp. 30-34.

Sterman, J. (2000) Business Dynamics. Irwin McGraw Hill. New York.

Wolf, F. (2001) “Operationalizing and Testing Normal accident Theory in Petrochemical Plants and Refineries” *Production and Operations Management*. Vol. 10, No. 3. pp.292-305.



**Dr. Hilda Blanco:** *Prioritizing Assets in Critical Infrastructure Systems*

**Christine Poptanich:** *Strategic Risk Analysis*

**Geoffrey S. French/Jin Kim:** *Threat-Based Approach to Risk Case Study: Strategic Homeland Infrastructure Risk Assessment (SHIRA)*

**William L. McGill:** *Techniques for Adversary Threat Probability Assessment*

**Michael R. Powers:** *The Mathematics of Terrorism Risk*

**Stefan Pickl:** *SOA Approach to the IT-based Protection of CIP*

**Richard John:** *Probabilistic Project Management for a Terrorist Planning a Dirty Bomb Attack on a Major US Port*

**LCDR Brady Downs:** *Maritime Security Risk Analysis Model (MSRAM)*

**Chel Stromgren:** *Terrorism Risk Assessment and Management (TRAM)*

**Steve Lieberman:** *Convergence of CIP and COOP in Banking and Finance*

**Harry Mayer:** *Assessing the Healthcare and Public Health Sector with Model Based Risk Analysis*

**Robert Powell:** *How Much and On What? Defending and Deterring Strategic Attackers*

**Ted G. Lewis:** *Why Do Networks Cascade?*

