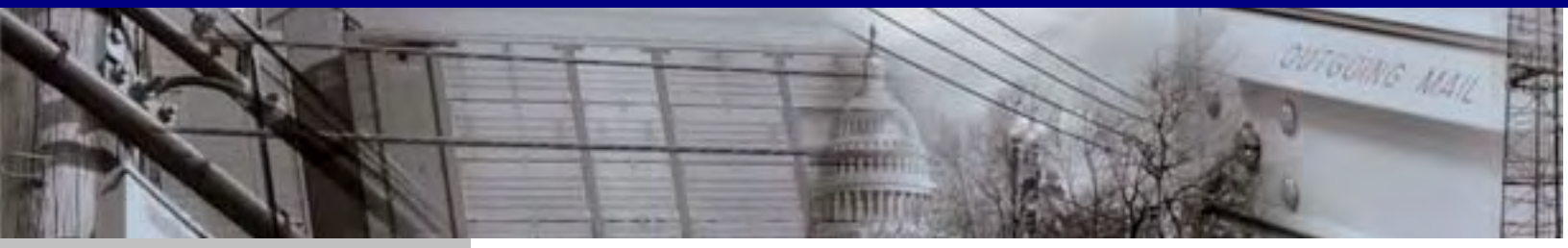
Critical Infrastructure Protection: *Elements of Risk*



Critical Infrastructure Protection Program

December 2007

GEORGE MASON UNIVERSITY

School of Law

CRITICAL INFRASTRUCTURE PROTECTION PROGRAM

Critical Infrastructure Protection: *Elements of Risk*

Critical Infrastructure
Protection Program

December 2007

Critical Infrastructure Protection Program

Mission

The George Mason University School of Law's Critical Infrastructure Protection (CIP) Program integrates law, policy, and technology to conduct comprehensive, nationally significant critical infrastructure research. The CIP Program provides critical infrastructure stakeholders in the National Capital Region with valuable analysis of the cyber, physical, and economic frameworks supporting the Nation's critical infrastructures. The core functions of the CIP Program are:

- Basic and applied research in critical infrastructure protection and security and defense issues;
- Timely and focused analysis of current issues;
- Convening critical communities for action; and
- Outreach and awareness for various stakeholders.

Background

After the critical infrastructure failures of September 11, the Federal government acted to fill gaps in the Nation's critical infrastructure preparedness. George Mason University's (GMU) location near the Nation's capital and its strong law and economics programs made it a natural base for performing critical infrastructure research. In 2002, Congress funded the creation of the CIP Project through the National Institute for Standards and Technology (NIST). Initially, the CIP Project performed basic and applied research on critical infrastructures. As the CIP Project matured, the quality and utility of the research attracted interest and funding from other agencies to explore new areas of critical infrastructure protection. Over the past five years, the CIP Project has evolved into the nationally recognized CIP Program through collaborations with NIST, the U.S. Department of Homeland Security (DHS), the U.S. Department of Energy (DOE), and other organizations throughout the region.

Accomplishments

The CIP Program has leveraged its substantial academic resources to enhance the preparedness, protection, and resilience of the Nation's critical infrastructure by leading scholarly discussion, promoting industry awareness, and providing support for public and private sector efforts. Leveraging its position as a third-party institution, the CIP Program has researched, assessed, and facilitated crucial public-private partnerships. By convening global leaders in areas such as law, telecommunications, insurance, and energy, the CIP Program has enhanced the dialogue between public and private stakeholders, and consequently advanced critical infrastructure protection. In addition, the CIP Program has assessed risk management in various sectors, analyzed interdependency issues facing the private sector, and produced a newsletter for critical infrastructure professionals. Ultimately, the CIP Program has become a national forum for exploring concepts that develops real-world solutions for protecting the Nation's critical infrastructure and key resources.

CIP Program Making a Difference

Basic and Applied Research

The CIP Program combines basic and applied research to produce relevant, actionable solutions to critical infrastructure protection problems. Among the many topics explored are cyber and physical security; information sharing between public and private sectors; regional, state, and local issues; energy; and privacy concerns. In particular, the CIP Program has researched critical infrastructure protection through prisms of law and economics, and this focused research has brought a rich branch of inquiry and knowledge to the national research agenda. For example, the CIP Program has advanced critical infrastructure economic modeling, and is developing measurable critical infrastructure metrics for the Federal government. To share research and exchanges ideas, the CIP Program has conducted numerous research symposiums and conferences to explore various topic areas. A broad range of research capabilities has helped the CIP Program engage the national and international community in addressing critical infrastructure protection.

Timely and Focused Analysis

The CIP Program produces timely and focused analysis of current issues, supplementing the basic and applied research with examinations and recommendations of topics relevant to critical infrastructure stakeholders. For example, the CIP Program surveyed the security and economic concerns of foreign investment in American technology and information infrastructures following the announcement of the Dubai Ports deal. In addition, the CIP Program has analyzed effective practices to secure vital systems and services provided by the region's critical infrastructures, and produced a framework for a National Capital Region Infrastructure Protection Plan.

The CIP Program has also analyzed energy risk mitigation and transfer, thus providing useful insight into insurance needs and governmental response to energy infrastructure destruction inflicted by the hurricanes of 2005.

Convening Critical Communities

The CIP Program partners public and private sector critical infrastructure stakeholders to produce innovative, actionable solutions to critical infrastructure protection challenges. The CIP Program has convened public officials and private sector members in various conferences and symposiums to address common interests. These meetings bridge the public and private sectors and grant a neutral location for all parties to examine complex issues. In addition, the CIP Program has specialized in private sector research and communication. GMU's academic strengths in law and economics are well situated to support public and private interests. In this capacity, the CIP Program's work has focused on legal, economic, business, and cultural solutions to enhance critical infrastructure protection through private initiatives and public work.

The CIP Program also connects state and local critical infrastructure communities with regional and national critical infrastructure populations. The CIP Program has

researched effective practices to secure vital systems and services provided by the National Capital Region's critical infrastructures. Much of the local research that the CIP Program has performed provides models for other communities to use. For example, the CIP Program has led focus groups for first responders, examined local interoperability issues, and convened national leaders with local critical infrastructure stakeholders to examine cross-cutting issues.

Outreach and Awareness

The CIP Program accomplishes outreach to and awareness for the critical infrastructure community in various ways. The CIP Program has published close to 300 articles, reports, and monographs on wide-ranging critical infrastructure topics. These publications have greatly contributed to the national dialogue on critical infrastructure protection, and have established the CIP Program at GMU as a leading source of critical infrastructure protection expertise. The publications range in topics from shared critical infrastructure functions and vulnerabilities, to *posse comitatus* and the military's role in disaster relief, to privacy and security.

In order to maintain awareness about critical infrastructure, the CIP Program generates a monthly newsletter (*The CIP Report*) that is read by public and private sectors, academia, international organizations, and other critical infrastructure stakeholders. *The CIP Report* engages and elicits positive feedback from the critical infrastructure community.

GEORGE MASON UNIVERSITY | School of Law

CRITICAL INFRASTRUCTURE PROTECTION PROGRAM

December 2007

As the phrase *critical infrastructure protection* (CIP) became familiar to many in the United States over the past decade, so has the term *risk*. Although neither CIP nor risk are new concepts, especially to those in the defense arena, they have gained significant traction in broader communities in recent years. With *risk* being increasingly used in discussions on homeland security, it is important to understand the fundamentals of risk and how it is managed on various levels. Thus, in an effort to promote a greater understanding of risk, the George Mason University School of Law's CIP Program is pleased to present this monograph entitled ***Critical Infrastructure Protection: Elements of Risk***.

The papers included in this monograph represent numerous perspectives on elements of risk and feature an array of authors working in the challenging field of homeland security. The papers address topics such as the definition of risk, assessment methodologies, and strategic approaches to risk management. Notably, the focus of this monograph is risk, and risk management, in the general sense. The monograph does not include papers delving into specific sectors, nor is it meant to endorse any one methodology or technology used in assessing and managing risk.

As explained by numerous authors, there is no common lexicon for risk management. This is largely due to the fact that both government and industry representatives are often working to manage, and mitigate, risk independent of each other. To frame the discussion, the following definitions from the U.S. Department of Homeland Security's National Infrastructure Protection Plan (NIPP) are noted:

> *Risk – A measure of potential harm that encompasses threat, vulnerability, and consequence. In the context of the NIPP, risk is the expected magnitude of loss due to a terrorist attack, natural disaster, or other incident, along with the likelihood of such an event occurring and causing that loss.*
>
> *Risk Management Framework – A planning methodology that outlines the process for setting security goals; identifying assets, systems, networks, and functions; assessing risks; prioritizing and implementing protective programs; measuring performance; and taking corrective action. Public and private sector entities often include risk management frameworks in their business continuity plans.*[1]

As stated above, this monograph is comprised of papers covering a range of topics, each of which lend to the broader discussion of risk as it relates to CIP. The papers are summarized below in the order of presentation.

In the first paper, entitled *Security Risk Management: Implementing a National Framework for Success in the Post-9/11 World*, Edward Jopeck and Kerry Thomas of the Security Analysis and Risk Management Association (SARMA) discuss the importance of a national strategy for security risk management. They acknowledge the Federal Government's intent to use a risk-based approach to CIP while noting that limited progress has been made in developing collaborative public-private efforts with regard to security analysis and risk management programs. The authors offer suggestions for improving security risk management processes and addressing other challenges in this growing field.

To elaborate on the first component of risk, threat, Geoffrey French of CENTRA Technology, Inc. addresses terrorism and threat analysis in his paper, *Intelligence Analysis for Strategic Risk Assessments*. Leveraging his current experience supporting the U.S. Department of Homeland Security, the author offers a valuable perspective on how threat information contributes to strategic terrorism risk assessments. He also discusses varying types of analysis, as well as their respective advantages and disadvantages. Importantly, French notes the need for both evidence-based threat assessments and imagination-based analysis to best inform decision-making on risk mitigation.

Delving even more into the technical side of assessing risk, the next three papers offer information on vulnerability, vulnerability assessment, and managing risk through network modeling. In *The Meaning of Vulnerability in the Context of Critical Infrastructure Protection*, William McGill and Bilal Ayyub of the University of Maryland explore ways to measure vulnerability and provide an operational definition for this component of risk. The authors offer mathematical expressions that detail two categories of vulnerability, protection vulnerability and response vulnerability. McGill and Ayyub also discuss how probability significantly impacts any assessment of vulnerability and, in turn, risk.

In *Vulnerability Assessment of Arizona's Critical Infrastructure*, Todd White, Samuel Ariaratnam, and Kraig Knutson describe the vulnerability assessment methodology used by the State of Arizona as an example of a state's approach to CIP. The authors' experience with the Phoenix (Arizona) Police Department / Arizona Counter Terrorism Information Center and Arizona State University position them to discuss the State's terrorism prevention program from numerous points of view. To delineate the many aspects of the program, they touch on issues such as data collection, training, layered screening for site evaluation, protection measures, and infrastructure design standards.

Managing Risk in Critical Infrastructures Using Network Modeling by Thomas Mackin of California Polytechnic State University and Rudy Darken and Ted Lewis of the Naval Postgraduate School illustrates the use of network analysis in a risk-based

approach to CIP. Specifically, Mackin, Darken, and Lewis describe critical node analysis as a means to determine the criticality of infrastructure components, i.e., nodes and links, and to calculate risk. Through an example of energy infrastructure, the authors demonstrate the value of critical node analysis in the identification and prioritization of critical infrastructure, and thus its utility to managing risk on a large scale.

Circling back to more strategic issues, the sixth paper in this monograph, *Same Words, Different Meanings: The Need for Uniformity of Language and Lexicon in Security Analysis and Risk Management* by Andrew Harter of SRA International, Inc., focuses on the need for a common lexicon in the field of security analysis and risk management. The author notes that the lack of consistently and commonly used terminology contributes to confusion among stakeholders and hinders collaboration. He outlines the process for developing standards, with considerable attention paid to the creation of voluntary consensus standards. Harter also offers detailed information on a SARMA project as one example of the efforts currently underway to establish a common lexicon.

Closing out the monograph, Robert Liscouski of Centurion Holdings, LLC and Nir Kossovsky of Steel City Re, LLC describe security as an intangible asset that requires dedicated attention from the corporate world in *The Intangible Value of Security in a Volatile Global Economy*. The authors assert that many companies have acknowledged the need to consider risk in their business practices and are affording greater consideration to enterprise risk management. Based on studies of the Intangible Asset Finance Society's Security Risk Management Committee, Liscouski and Kossovsky recommend that stakeholders use a process of five steps to enhance their security risk management and expound on each step with guidance for improving current practices.

Combined, these seven papers offer a wealth of information on risk, to include examples of current risk management practices and efforts aimed at better protecting the Nation's critical infrastructure. It is hoped that these papers contribute to present discussions on risk and spur additional dialogue on this important theme of homeland security.

[1] U.S. Department of Homeland Security, *National Infrastructure Protection Plan*, June 2006, p. 105.

Table of Contents

Security Risk Management: Implementing a National Framework for Success in the Post-9/11 World

Edward J. Jopeck and Kerry L. Thomas

Abstract: Recent legislation, national strategies and the public statements of senior government officials all call for the use of **risk management** as the cornerstone of the Nation's effort to protect its critical infrastructure and to inform decision-making in Homeland Security. Few would disagree with this objective. However, the General Accounting Office, Congressional Research Service, and numerous insightful observers have all noted the lack of progress in security analysis and risk management programs. Now, more than 6 years since the 9/11, there appears to be a large and growing gap between what policy makers need, and what the security analysis and risk management community is currently able to provide. This article will explore the causes of this gap, identify obstacles to progress, and explore initiatives still needed to achieve the goals sought by Congress, the Executive Branch, and the American public.

Over the past several decades, significant resources have been expended by Federal departments and agencies, as well as in the private sector, to implement more uniform and rigorous security risk management processes and methods. However, despite the considerable sums spent to effect change, security risk management efforts 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 use by the profession, 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, other Federal agencies, and the private sector 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 with measurable results for intelligently reducing the risks associated with terrorism.

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 necessary 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 practitioners with similar missions. This article attempts to identify the primary reasons for the apparent lack of progress, and explores a vision for implementing a more successful risk management program that can provide the Nation with 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, the success of prior efforts has often been limited because they did not address the fundamental building blocks needed to establish the basis for success. Figure 1 below illustrates this in more detail.

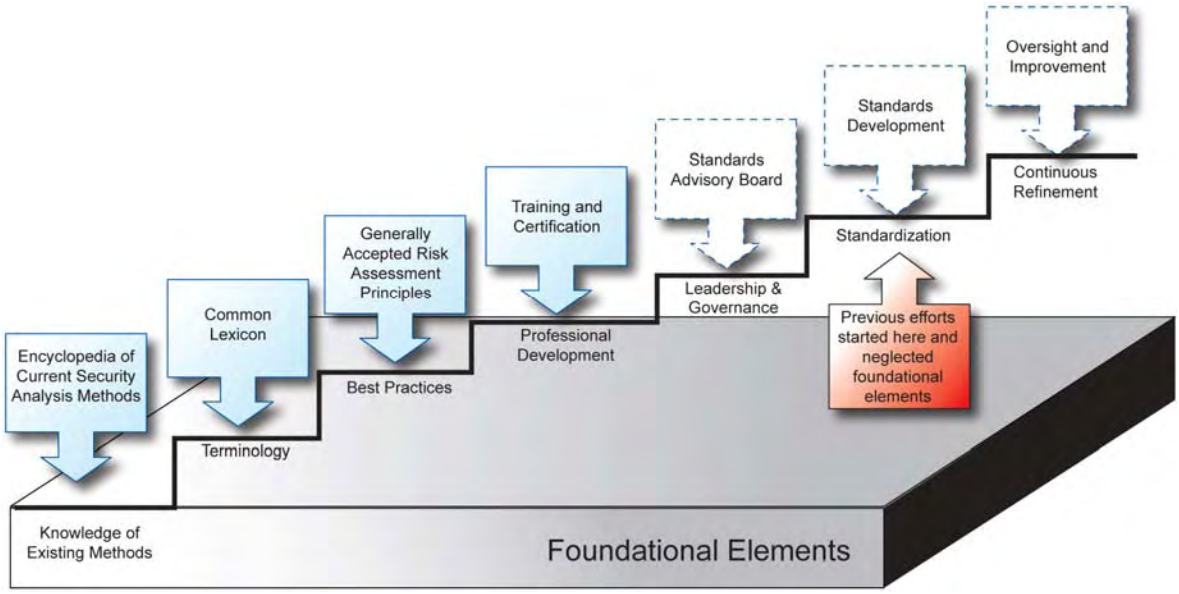


Figure 1. Creating the Foundation of Security Risk Management - The Building Blocks of Success

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 currently in use are not based on recognized or compatible metrics, the resulting data is often useless to others who 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 between the Federal Government, State and local governments, and the private sector. While many attempts to dictate standards within individual Federal departments and agencies have been made, their conflict with similar efforts elsewhere only exacerbates the problem. Without a common language for use 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-07-386T

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 Laboratories, the private sector, and academia has developed. The resulting free-for-all has slowed progress on this issue to a virtual standstill.

As long as each effort stands alone, synchronization of methods and the ability to validate the conclusions of the resulting assessments is not possible. One powerful example of the impact of such fragmented efforts is that, since 2001, over $12 billion[1] 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 International) has begun developing its own risk management standard to fill the void in federal security efforts. Even international organizations, such as the Risk Management Institution of Australasia Limited (RMIA), have stepped in to fill the void with efforts to document a common body of knowledge for security risk management. As such grass-roots movements gain momentum, the Federal Government risks losing the ability to shape the future of security risk management and ensure that its own needs can be met.

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 profession requires strong leadership, a bold vision for coordinated governance, and a comprehensive plan to implement the partnerships necessary for a ***national strategy*** for security risk management. The past two decades have shown that the "every entity for itself" approach will not result in a coordinated national effort, as doing so is beyond the mission and authority of any one organization. The U.S. Government Accountability Office (GAO) and Congressional Research Service (CRS) have both come to recognize this may indeed be the case. In a December 2005 report on homeland security risk management, GAO concluded:

> *[F]or 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.*[2]

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.*[3]

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 NSPD/HSPD 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:

  - ***Security Advisory and Risk Standards Board (SARSB).*** The 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 governments, the private sector, professional associations, and academia to translate the architecture into a roadmap for implementation.

    - Be the Federal Government's authority on security risk management, with responsibility for collecting lessons learned from past efforts and developing voluntary consensus standards for terminology, generally accepted principles for risk assessment, and 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 having disagreements over security risk management activities and policies that may affect national/homeland security interests.

- *Interagency Risk Management Support Staff* (IRMSS). The function of the 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 to security risk management. 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 Security Risk Management Program by providing tailored training and assisting in program development.

  - Produce educational multimedia products and present on the program at conferences for the homeland security, defense, intelligence, and public safety communities.

  - Help Federal, State, and local governments 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 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 necessary policies and procedures and leads risk management initiatives at the department and/or agency-level. Of

note, we believe the initial focus of this position should be on coordination of security risk activities; however, the ultimate goal should be a convergence of all risk activities within the CRO's portfolio.

- **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 for the development of a coordinated security risk management strategy must also include active partnerships with the security industry to achieve the goals and objectives of 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 public 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 SARMApedia effort. The initial focus of the SARMApedia 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, several specific projects have 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 **Who's Who in Security Analysis Project** is developing a listing of individuals and organizations that will enable policy-makers, practitioners, and

researchers find the expertise they need from within the profession. It will also provide practitioners and organizations with the opportunity to share their expertise, interests, and accomplishments with their peers.

- The **Research and Development in Security Analysis Project** is developing a listing of projects and research needs that will allow government sponsors, practitioners, and researchers to know where focused research exists, where efforts are redundant, and where gaps in research and development efforts still exist.

- 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 SARMApedia 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 risk practitioner. Even with visionary leadership and direction it will not be easy, as GAO 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 with the security it needs at a price it can afford.

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, defense and homeland security communities. Between 2003 and 2007 he served as a security risk management consultant to the U.S. 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 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.

[1] Congressional Research Service, *The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress*, Order Code RL33858, February 2, 2007, p. 27. Available at http://www.fas.org/sgp/crs/homesec/RL33858.pdf, accessed September 25, 2007.
[2] 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, December 2005, p. 109. Available at http://www.gao.gov/new.items/d0691.pdf, accessed September 25, 2007.
[3] Congressional Research Service, *The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress*, Order Code RL33858, February 2, 2007, pp. 25-26. Available at http://www.fas.org/sgp/crs/homesec/RL33858.pdf, accessed September 25, 2007.

Intelligence Analysis for Strategic Risk Assessments

Geoffrey S. French

Abstract: For the critical infrastructure protection community to implement a risk-based prioritization of resources — whether at the facility, community, or other level — it requires information about the threats, vulnerabilities, and consequences of a variety of potential scenarios. Comprehensive information on the terrorist threat can only come from the government. Strategic terrorism threat assessment, however, is particularly challenging for the U.S. Intelligence Community because it requires a degree of prediction and communication with the public — both of which run counter to the community's culture. To form a basic strategy for reducing the risk from terrorist attacks, decision-makers need (1) evidence-based threat assessments to provide comparative analysis of a range of adversaries and attack methods, and (2) imagination-based analysis to give them alternate perspectives on the threats they face, including information on the ways that the terrorist threat may change.

INTRODUCTION

The perfect system for translating information on terrorist groups into threat analysis useful for strategic terrorism risk assessments has yet to be developed. Difficulties permeate the process, beginning with the sustained information-sharing required for the consolidation of all pertinent intelligence into one place. The small numbers of past attacks in the United States lend themselves to poor extrapolation. Similarly, broad conclusions based on tactical intelligence introduce uncertainty into the analysis. Finally, the application of intelligence into coherent, quantified analysis for risk assessment requires a logical structure to capture analytic judgments. It is important for decision-makers to understand the difficulties that strategic terrorism analysis poses for the U.S. Intelligence Community (IC) and the purpose of the various types of analysis that exist. 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.

TERRORISM AND INTELLIGENCE ANALYSIS

Although terrorism is not a new phenomenon, its centrality in the IC is, as are the heightened demands for communicating intelligence assessments outside of the IC. Similarly, the need for intelligence to be put into a context for risk analysis is also relatively new. The IC is restructuring its organizations and culture to meet these needs, but the process is incomplete. The reason is largely due to the IC's historical approach to analysis. Understanding the inherent challenges in providing strategic

warning and the similarities that it shares with terrorism threat analysis helps provide context for the difficulties of framing threat for risk assessments.

Strategic Warning

The IC as presently conceived was formed largely during World War II and matured in the Cold War. At its best in this period, it focused intelligence collection and analysis on specific questions having to do with military, political, and economic issues. Assessing the current state of foreign programs or affairs and short-term outlooks were clear tasks, and the IC excelled at finding innovative approaches to penetrate closed societies, discover secret programs, and exploit human intelligence. The legacy of the attack on Pearl Harbor brought another set of expectations, however, that the IC would help the nation avoid strategic surprise.[1] The demand for long-term outlooks and predictions of major shifts that necessitate swings in national strategy or a change in governmental priorities, however, did not fit the IC's approach and expertise well.

The shoals of strategic warning are difficult to navigate. Analyses that predict major change in the long term — or even the near term — are inherently uncertain and liable to be erroneous. To have any utility, however, such predictions must be delivered with sufficient time for government officials to change policy of programs. Issuing the analysis before clear evidence exists invites criticism for lacking credibility; waiting for clear evidence, in contrast, means delaying until the analysis is no longer useful. The needs for timeliness and credibility, therefore, work at cross-purposes.[2] Moreover, experts tend to be poor forecasters. Numerous studies have shown predictions by experts in specific fields to be no better than simple statistical models.[3] All of these factors combine to make strategic warning among the most difficult tasks the IC faces. Unfortunately, strategic terrorism threat analysis more closely resembles this task than the others.

Strategic Terrorism Threat Analysis

Clearly, the IC plays a broad role in counter-terrorism. The IC is central to the task of identifying, monitoring, and intercepting terrorist planners, operatives, and their support networks, including financial analysis. The IC plays a pivotal role in denying terrorists access to weapons, material, and targets, including non-proliferation and tracking sensitive material. The IC also assists the U.S. military in targeting (such as locating training camps or identifying, intercepting, and translating communications) and force protection. IC support to force protection is directly applicable to risk analysis. By providing threat analysis, the IC allows the U.S. military to shift resources, change defensive tactics, move units or equipment, or eliminate the threat.

The U.S. critical infrastructure community requires threat analysis for similar reason. To make informed decisions about how to adjust protective measures or invest in preparedness measures, the community needs a better understanding of the threat. When tactical intelligence is available, its application is relatively straightforward. If a

terrorist cell or individual has been identified and penetrated, the target of the attack (e.g., John F. Kennedy airport or Ft. Dix) can be ascertained. If the cell is capable of launching the attack, the authorities may arrest the members and eliminate the threat or increase protections around the target to reduce vulnerability. If analysis indicates that the consequences of the attack would be very low, the cell may be allowed to operate while authorities attempt to find links to other groups or planners. In the absence of explicit tactical information, however, the critical infrastructure protection community still requires an input for threat into the risk model. *Strategic* terrorism threat assessments support risk management of long-term problems or for multi-year outlooks.

Modern terrorism presents a very different challenge than the nation state — focused efforts that have dominated the history of the IC.[4] First and foremost, there is no structured command and control system to penetrate. The highest tiers of an international terrorist group may not issue specific tactical orders on targets or attack methods. Cells in the United States may simply be inspired by the al-Qa'ida ideology and generate their own concepts of where and how to attack. Even if U.S. authorities intercepted every communication between a U.S. cell and the central al-Qa'ida leadership, they may have little insight into the details of the plot. In this way, strategic terrorism analysis meets Gregory Treverton's definition of a mystery, as opposed to a puzzle.

> *Puzzles can be solved; they have answers. But a mystery offers no such comfort. It poses a question that has no definitive answer because the answer is contingent; it depends on a future interaction of many factors, known and unknown. A mystery cannot be answered; it can only be framed, by identifying the critical factors and applying some sense of how they have interacted in the past and might interact in the future. A mystery is an attempt to define ambiguities.*[5]

This inability to provide definitive answers puts the IC in a conundrum. For its anti-terrorism mission, the best outcome is to deliver clear information about threat to the public with enough time to prepare for an attack. Absent tactical threats, this requires the IC to either make predictions or to provide some insight into how and what terrorists may attack. All of this runs counter to the culture of the IC.[6] For this reason, much of the IC analysis that has been released to the public has been tactical in nature (e.g., there is or is not a threat to an event or facility[7]) or very high level (e.g., al-Qa'ida continues to pose a threat to U.S. interests[8]).

Threat Analysis for Risk Management

Unfortunately, these types of analysis do not meet the needs for risk management. For decision-makers to implement a risk-based prioritization of resources — whether at the facility, community, or other level — they require information about the threats, vulnerabilities, and consequences of a variety of potential scenarios. Information about vulnerabilities and consequences can often be obtained from the owner or operators of key facilities or from an outside expert. All-inclusive information on the terrorist threat, however, can only come from the government. Tactical analysis can

help inform decision-makers about an individual threat, but it does not help set longer-term priorities or help invest resources for much beyond the immediate term. Analysis at too high a level does not provide the comparison of multiple adversaries and multiple types of attack scenarios required to discriminate good investments from poor. Similarly, analysis with too narrow a focus can hinder strategic decision-making; for example, an in-depth evaluation of al-Qa'ida's capability to use chemicals in an attack may be informative for assessing an individual scenario, but does not help determine whether a community needs HAZMAT gear more than an augmented bomb squad.

To form a strategy to reduce the risk from terrorist attacks, decision-makers need a threat assessment based on intelligence and supporting evidence so that they can compare the severity of several threats, understand the degree of certainty in the assessment, and determine the potential for change. With these elements identified, decision-makers would have a credible system to apply to risk analysis. Credibility, however, is only one of the aspects of strategic warning. Ideally, the government can offer imagination-based analysis to complement the evidence-based analysis and give decision-makers timely insight into other perspectives on the threats they face, including information on the ways that the terrorist threat may change. Aspects of both of these approaches are described below.

EVIDENCE-BASED ANALYSIS

As mentioned above, strategic risk analysis must take multiple unwanted events or hazards into account. To compare these, it requires a consistent approach that can differentiate the adversaries and multiple types of attack scenarios meaningfully, whether by frequency or severity. This differentiation may simply be qualitative (low, medium, or high) but for a broad range of attack types and potential targets, three or even five categories will leave most scenarios clustered in a narrow band. To maximize its utility for risk management, threat analysis should have judgments that can be represented numerically. Unfortunately, obtaining the evidence and quantifying it is no simple task and has led to missteps in the past (see Box 1).

To frame the quantification, many systems attempt to produce a probability or at least a proxy for probability. Many probabilistic risk systems for terrorism resemble models created for safety risk analysis. The mechanical and nuclear engineering fields have a generally successful model for probability based on knowing the number of times that a part or process will fail in its lifetime due to fatigue, stress, breaks, or errors. Even complex processes can be evaluated in this fashion by breaking them into their constituent parts and then evaluating and aggregating their probabilities. The fundamental problem with applying this approach to terrorism risk analysis is the unknowable probability that a nation, city, or facility will be attacked in a given period of time.

Outside of having information on a specific terrorist cell, the IC and law enforcement community rarely have enough information to know that an attack is imminent or set for a specific timeframe. Another way of approaching the problem is to consider the

events in Washington D.C. between September 2001 and October 2002. The metropolitan area experienced the attack on the Pentagon, anthrax sent through the mail, and a serial sniper. Individually, these events do not lead to any conclusion about the number of terrorist attacks that Washington D.C. should anticipate experiencing within the next year. Taken out of their context and treated collectively, they would lead to the illogical conclusion that Washington D.C. should expect three attacks over whatever timeframe is selected (one year, five years, ten years, etc). Some terrorism risk models, therefore, use a conditional probability that assumes an attack within a certain timeframe and focuses on attempting to assess its potential form and its target.

Box 1: The Pitfalls of Quantification

Many threat analysis systems confuse the need for quantified results with a blind search for numbers. Some recent threat analysis approaches have been based on easily counted proxies, such as the number of open terrorism investigations or suspicious activity reports.[9] This has an appeal in that the numbers are verifiable and quantifiable. It ultimately fails because the proxies do not reflect the aspects of the information that actually indicate threat or maturity of the cell, what are its capabilities, what may be the intended target. Worse, they are significantly influenced by the enthusiasm of those submitting suspicious activity reports and the standards of recording them. Similarly, the last six years have seen construction of several databases that include information on terrorist incidents worldwide. One intention behind these databases is to collect enough data to be able to calculate statistical probability. Like the number of open terrorism investigations, databases have something to contribute to the understanding of threat, but statistical analysis is ill founded. By equating the security environments in nations around the world and the terrorist attacks from groups with very different intentions and goals, databases can lead to poor conclusions, such as that only 1 percent cause fatalities.[10] This may be true for a database with tens of thousands of incidents but provides no meaningful understanding of the threat to decision-makers in the critical infrastructure protection community.

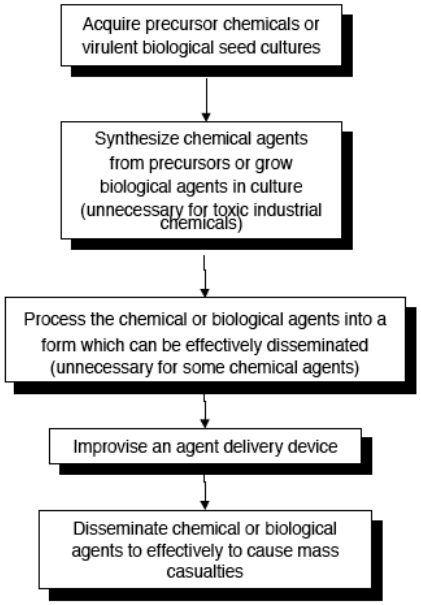
Regardless of the model's context for the quantification, the output from a strategic threat assessment must succeed on two counts to be useful for risk management. It must communicate distinct threat levels for multiple scenarios and it must allow managers to understand what evidence was considered and how it affects the results. There are two principal approaches that hold promise for risk management: event tree analysis and threat severity analysis.

Event Tree Analysis

One approach to threat analysis is to identify all of the required actions for an adversary to launch an attack and to assign probabilities to each step. This is typically referred to as an event tree or an attack tree. To illustrate, Figure 1 shows the basic actions required for chemical or biological terrorism. To translate this into an attack tree, an analyst would select a specific chemical or biological agent and a

target to create a scenario. One benefit of such an approach is that it reveals potential indicators of an attack or signatures that a terrorist cell may have, and thus likely places for detection and interdiction. To use this approach to generate a quantified threat level, the analyst must additionally assign probabilities for success for each step. For some weapons or agents, acquiring precursor materials may have a very low percentage of success, which could reflect controls on specific materials, treaties in place, or other law enforcement mechanisms that make this step difficult. Probabilities for the synthesis or growth of agents and weaponization of the agents may be based on the difficulty of working with the specific material, but assumptions of the skill level of the terrorist group in question also underpin the analysis. Similarly, assumptions about target selection and vulnerability, as well as the ability of U.S. intelligence or law enforcement agencies to interdict the attack, are also implicit in the probability of the successful dissemination of the agents. Multiplication of all of the probabilities provides an overall threat level.

Figure 1: An Event Tree Analysis Based on Stages for Terrorists Working Outside a State-run Laboratory to Conduct Chemical and Biological Terrorism.



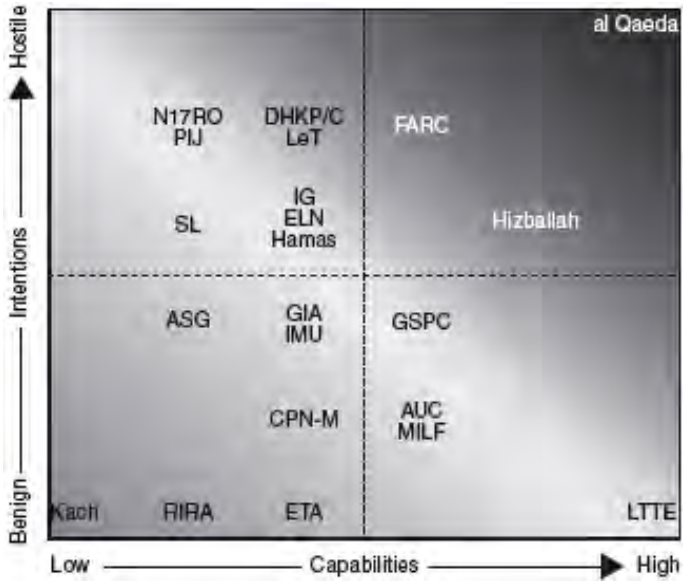
Source: U.S. General Accounting Office, *Combating Terrorism: Need for Comprehensive Threat and Risk Assessments of Chemical and Biological Attacks*, GAO/NSIAD-99-163, September 1999, p. 8.

This type of threat analysis requires extensive documentation of the assumptions that were considered in each step and of how the probabilities were generated. Without these, the process is difficult to repeat with confidence that it will produce consistent conclusions. Moreover, even small changes in the probability of any step can result in very different risk levels when other elements of vulnerability and consequence are combined with it. It does, however, have the advantage of being clear in its components and can be useful in generating quantified threat levels that can help to compare threats and contribute to risk analysis.

Threat Severity Analysis

Another established approach to assessing the threat from an adversary is to identify the adversary's capability to launch an attack and the overall intent for that adversary to do so. Figure 2 illustrates a comparison of several terrorist groups based on these two criteria and demonstrates the potential utility of threat severity analysis. The benefit of such an approach is that it can create a set of definitions to mark various levels of capability and intent and communicate these to a wide audience. By combining the levels of capability and intent, the system can communicate the severity of the threat to decision-makers. It should be clear, for example, how a group with a high intent may actually pose a more immediate threat than one with greater capability. Although the approach is sound, it still does not provide sufficient detail to the critical infrastructure protection community for risk analysis in that it does not differentiate various types of attack methods for the groups or the intent as applied to specific targets. A strategic risk assessment requires a threat analysis for a range of scenarios that "consist of target assets, weapons, and modes of delivery."[11]

Figure 2: Threat Severity Analysis Using Intent and Capability Levels for Multiple Terrorist Groups.



Source: Kim Cragin and Sara A. Daly, *The Dynamic Terrorist Threat*, RAND: Santa Monica, CA, 2004, p. 20.

Specifically, a threat analysis system would require an assessment of capability for a range of attack methods (such as the use of chemical agents, biological agents, and explosives). It also requires as assessment of intent to attack individual facilities or general types of assets with each of those attack methods. Ideally, intent levels reflect the adversary interest in attacking a class of assets in general (e.g., government buildings) as well as any specific interest in using an individual attack method against a specific target (e.g., using a vehicle-borne improvised explosive device against a federal government headquarters building). The analysis of intent is

particularly difficult. Too often, analysts attempt to extend lessons learned into universal statements about terrorist preferences for targets or attack methods. This can lead to illogical conclusions, especially with poorly defined terms such as "soft targets." There are situations in which terrorists have clear preferences for targets that are constant over time; it is equally clear that some terrorist planners consider certain vulnerabilities or consequences and use them to guide the selection of targets.[12] Even so, some targets are highly vulnerable and an attack on them could have severe consequences, yet they are not considered to be a priority for terrorists.[13] Analysis of intent, therefore, needs to be painstakingly researched to document the judgments about terrorist preferences and potential targets. The opposite approach — crafting general statements of what terrorists find "attractive" — will most likely lead to false positives and false negatives.[14] A system that can illustrate capability levels for a series of attack methods and the related intent levels for classes of targets and geographic regions would enable risk management across a sector, in a city or region, and at the facility or system level. This would provide useful distinctions among the threat for scenarios that combine the attacker, a method of attack, and the attack's target.

Other Approaches

The categories above do not capture the full spectrum of approaches to threat analysis. Some models, for example, use Bayesian networks to calculate probabilities for terrorist attacks. These have the appeal of adhering to logical rigor because there is a defined probability space (where an increased probability of one attack means decreased probability of another) and intended ratio relationships (where a probability of 0.4 is four times as likely as 0.1). The level of detail required for such systems, however, is impractical to support with intelligence and ultimately depends on subjective judgments.[15] These complex models can be useful as internal tools for an organization, but do not provide the credibility for outside validity and implementation across a large number of organizations.

Conversely, a simplistic approach to threat analysis is a "scorecard" method that tallies various contributors to a threat, such as ease of access to the materials or expertise for the attack, or the symbolic value of the target (see Figure 3). These are simple to understand and can be implemented by people with little security training. More complicated versions do exist,[16] but ultimately these offer a proxy for threat — just as a material threat assessment does — by attempting to estimate the logistical burden of an attack, not the capability or intent of an adversary.

Figure 3: A Scorecard Approach to Threat Assessment.

	Criteria						
Scenario	Access to Agent	Knowledge/ Expertise	History of Threats (Building Functions/ Tenants)	Asset Visibility/ Symbolic	Asset Accessibility	Site Population/ Capacity	Collateral Damage/ Distance to Building
9-10	Readily available	Basic knowledge/open source	Local incident, occurred recently, caused great damage; building functions and tenants were primary targets	Existence widely known/iconic	Open access, unrestricted parking	> 5,000	Within 1,000-foot radius
6-8	Easy to produce	Bachelor's degree or technical school/ open scientific or technical literature	Regional/State incident, occurred a few years ago, caused substantial damage; building functions and tenants were one of the primary targets	Existence locally known/ landmark	Open access, restricted parking	1,001-5,000	Within 1-mile radius
3-5	Difficult to produce or acquire	Advanced training/rare scientific or declassified literature	National incident, occurred some time in the past, caused important damage; building functions and tenants were one of the primary targets	Existence publish/well-known	Controlled access, protected entry	251-1,000	Within 2-mile radius
1-2	Very difficult to produce or acquire	Advanced degree or training/ classified information	International incident, occurred many years ago, caused localized damage; building functions and tenants were not the primary targets	Existence not well-known/ no symbolic importance	Remote location, secure perimeter, armed guards, tightly controlled access	1-250	Within 10-mile radius

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

IMAGINATION-BASED ANALYSIS

Evidence-based systems alone cannot provide all of the insight that decision-makers need to consider threat. Their value is that they can show how the weight of evidence influences judgments about the severity of a threat. Their weakness is that the dependence on past events and clear indications of capability or intent will prevent them from providing timely insight into sudden or more radical shifts in the threat that require more innovative approaches to identify. Imagination-based analysis frees an analyst from the constraints of a structured model and complements the insight that evidence-based systems provide. Red Cell analysis, Red Team exercises, and game theory are three established approaches to this less structured area of threat analysis.

Red Cell analysis is specifically intended to question the underlying assumptions of the evidence-based analysis and pursue alternative hypotheses. Red Cell analysis

has a greater degree of flexibility in interpretation of events, information, and intelligence. By examining them from different perspectives or combining certain facts differently, Red Cell analysis informs decision-makers by revealing uncertainties or questionable assumptions in any evidence-based analysis and emphasizing the continuum of possibilities for threat, specifically where it may be higher than thought or where opportunities for strategic surprise exist (see Box 2).

Box 2: An Example of Red Cell Analysis

In 2002, the National Infrastructure Protection Center (NIPC) evaluated trends in terrorism. These included an increase in operational complexity, an interest in new forms of attack, and an increase in infrastructure as a target for attack. Given the increase in physical countermeasures after the September 2001 terrorist attacks, the NIPC analysts speculated that terrorist may attempt to use cyber attacks to overcome some of the constraints on physical access or to increase the destructiveness of their physical attacks.

Since that time, it is clear that the terrorist threat has changed. Attacks in Western Europe have become simpler, not more complex, and terrorist groups rely more heavily on suicide attacks than on technological adaptation. Regardless, this analysis offered an innovative assessment of how the terrorist threat may develop that may have caused risk managers to reduce key cyber vulnerabilities.

Source: National Infrastructure Protection Center, *Swarming Attacks: Infrastructure Attacks for Destruction and Disruption*, July 2002.

A related but distinct analytic approach is the Red Team. Red Teams typically run exercises or tests of security in the field. Red Teams, like Red Cells, offer the opportunity to validate or contradict the assumptions made in threat analysis: whether a target is identifiable, whether certain defensive configurations deter surveillance, and whether material for an attack is easily obtained (see Box 3). Red Teams are most effective at analyzing a persistent threat, where the adversary is fixed on one target and searches for innovative means of overcoming the countermeasures in place. Red Teams can also help assess threats that may fall outside of a modeling construct for evidence-based analysis.

Both Red Cells and Red Teams can use game theory as an approach to analysis or exercises. Game theory is another mechanism for exploring the dynamic nature of threat and its relationship to vulnerability, consequence, and terrorist goals. A static model for risk is — as all models are — an artificial construct to assist people in comprehending a problem and gaining insight into potential solutions. These simple models are very useful but must be complemented by other means, such as game theory, in order to add another dimension to the understanding of threat. Game theory can accommodate a nuanced and complex approach to terrorist intent and target selection.

Box 3: An Example of Red Team Analysis

In 2007, the U.S. Government Accountability Office conducted an investigation into the safeguards on the purchase of radioactive materials. The investigation took the form of a Red Team that established a bogus business to obtain a radioactive materials license from the Nuclear Regulatory Commission. After receiving the license, the investigators altered it to allow the purchase of an unrestricted quantity of radioactive sources and successfully used it in the acquisition of machines containing radioactive material.

This investigation tested the countermeasures in place to prevent unauthorized personnel from obtain material that could be used in a radioactive dispersal device. By demonstrating the vulnerabilities, the Nuclear Regulatory Commission was able to correct the weaknesses identified in the exercise.

Source: U.S. Government Accountability Office, *Nuclear Security: Actions Taken by NRC to Strengthen Its Licensing Process for Sealed Radioactive Sources are Not Effective*, GAO-07-1038T, July 12, 2007.

Game theory is best utilized in examining an adversary that is pursuing a type of effect (e.g., mass casualties) rather than a specific target (e.g., a federal government building). The adversary is free to change targets and tactics based on site-specific countermeasures, general changes in security posture, or other obstacles. Military war games that focus on Effects-Based Operations provide an excellent example of a system to model such dynamic agents.[17]

Imagination-based analysis provides the best opportunity for the IC to provide timely warning about the potential shape of the future terrorist threat. If the IC can engage in an on-going dialogue where this type of analysis complements a systematic evidence-based threat model, it should be able to balance the needs for timeliness and credibility. By using risk management as the long-term framework for discussion, the IC and CIP communities should be able to explore future permutations of the threat without accusations of crying wolf or scare mongering.

CONCLUSIONS

The current state of strategic terrorism threat assessment does not support proper risk management in the critical infrastructure realm. Attempts at threat analysis for use in the private sector have been at the wrong level or relied too heavily on imagination-based analysis. Although imagination-based analysis can inform the decision-making process, it is a challenge for decision-makers to use it as a basis for investments or action. Even the best imaginative work carries a high degree of uncertainty. Risk management must begin with a strategic, evidence-based threat analysis.

Members of the critical infrastructure protection community — state and local governments, owners and operators, and federal agencies with security responsibilities — need to be specific in their requests for threat analysis. Typically, the IC provides tactical warnings and periodic updates on the threat environment

from a high-level perspective. These types of communication are worthwhile, but do not provide the comprehensive outlook required to make investments in a strategic plan for a facility, infrastructure sector, or community. Only a comparative, evidence-based threat analysis can serve as the foundation for an informed risk management strategy.

The IC needs to acknowledge the criticality of threat analysis to risk management. Without threat input to risk, the private sector develops workarounds, either generating it itself or using methods like CARVER. CARVER — an approach to target selection developed by U.S. Special Forces — does help a decision-maker understand how a system may be attacked or which of a series of assets may be attacked.[18] It does not, however, compare threat levels across multiple attack methods or types of weapons. This minimizes or can misrepresent the threat factor in risk calculation and can skew the analysis toward attacks for which there is no intelligence or other indication that terrorists have any interest in pursuing. Ultimately, this can lead to poor investment decisions that overlook mitigation strategies for more likely contingencies.

Both the IC and the critical infrastructure protection community need to recognize the inherent difficulties in the strategic terrorism threat analysis process and work together to implement a realistic system for providing and safeguarding threat information. The communities need to take multiple approaches to the problem of using strategic intelligence for threat analysis and develop multiple tools to allow them to view threat from different perspectives. The critical infrastructure protection community must understand that strategic warning is more of a mystery than a puzzle, and that ambiguities will always remain. The IC needs to put a greater priority on communicating threat information in a way that enables better risk management. Only by sustained engagement with the critical infrastructure community will the IC fulfill its mandate for providing strategic warning that is both timely and credible.

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 worked in counterintelligence and in the critical infrastructure protection community since the 1990s, supporting government agencies such as 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.

---

[1] John Ranelagh, *The Agency: The Rise and Decline of the CIA* (Simon and Shuster: New York, 1987), p. 55.
[2] Jack Davis, "Improving CIA Analytic Performance: Strategic Warning," The Sherman Kent Center for Intelligence Analysis Occasional Papers: Volume 1, Number 1, September 2002, p. 3.
[3] Rob Johnson, *Analytic Culture in the U.S. Intelligence Community* (Government Printing Office: Pittsburgh, Penn., 2005), p. 64; Richard K. Betts, "Fixing Intelligence," *Foreign Affairs* January/February 2002, p. 49.

[4] It is also important to contrast the modern al-Qa'ida modus operandi of clandestine groups willing to kill themselves in support of attacks that maximize destruction with that of other groups and earlier operations where the terrorists intended to keep themselves alive and often gave warnings about imminent attacks.
[5] Gregory F. Treverton, "Risks and Riddles" *Smithsonian* June 2007, p. 98.
[6] For difficulties facing information-sharing in particular, see James B. Steinberg, Mary Graham, Andrew Eggers, "Building Intelligence to Fight Terrorism," The Brookings Institution, September 2003, p. 2.
[7] Statement By Secretary Chertoff on London Incident, June 29, 2007, http://www.dhs.gov/xnews/releases/pr_1183129350044.shtm; Statement by Homeland Security Secretary Michael Chertoff on the Bombings in Mumbai, July 11, 2006, http://www.dhs.gov/xnews/releases/press_release_0949.shtm; Remarks by Secretary of Homeland Security Tom Ridge at a Press Conference Announcing the Raising of the National Threat Level, December 21, 2003, http://www.dhs.gov/xnews/releases/press_release_0889.shtm.
[8] Declassified Key Judgments of the National Intelligence Estimate, "Trends in Global Terrorism: Implications for the United States," April 2006 www.dni.gov/press_releases/Declassified_NIE_Key_Judgments.pdf; Declassified Key Judgments of the National Intelligence Estimate, "The Terrorist Threat to the US Homeland," July 2007, www.dni.gov/press_releases/20070717_release.pdf.
[9] Todd Masse, Siobhan O'Neil, and John Rollins, "The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress" (Congressional Research Service, February 2007), p. 11.
[10] Jeanna Bryner, "New Database Debunks Terrorism Myths," LiveScience, May 24, 2007, http://www.livescience.com/history/070524_terrorism_database.html.
[11] Gregory S. Parnell, Dr. Robin L. Dillon, and Terry Bresnick, "Integrating Risk Management with Homeland Security and Antiterrorism Resource Allocation Decision-Making" in *The McGraw-Hill Homeland Security Handbook* (New York: McGraw Hill, 2005).
[12] Tom Hays, "NYPD says al-Qaida Operative Favored Limo Bomb for U.S. Targets," The Associated Press, November 16, 2006.
[13] Simon Cox, "U.S. Food Supply 'Vulnerable to Attack,'" BBC News, August 22, 2006.
[14] As an example, consider the "balanced scorecard," which considers terrorist "return on investment" such as loss of life, increase in Islamic presence, and decrease in Western presence, among other factors, in its threat analysis. The system assigned probabilities of 77.93% for U.S. embassies and 0.00% for transportation assets. Although these are extant threats to U.S. embassies, these probabilities are incongruous with recent terrorist attacks on Western targets. See G.A. Beitel, D.I. Gertman, and M.M. Plum, "Balanced scorecard method for predicting the probability of a terrorist attack," in *Risk Analysis IV* (Southampton, UK: WIT Press, 2004), p. 589.
[15] For a discussion of the type of structured analysis that may allow Bayesian analysis, see J. McLaughlin and M.E. Patè-Cornell, "A Bayesian Approach to Iraq's Nuclear Program Intelligence Analysis: A Hypothetical Example," presentation at the 2005 International Conference on Intelligence Analysis, McLean, VA, May 2, 2005.
[16]Martin M. Plum et al., "Novel Threat-Risk Index Using Probabilistic Risk Assessment and Human Reliability Analysis" (Idaho National Engineering and Environmental Laboratory, February 2004).
[17] Lee W. Wagenhals and Larry K. Wentz, "New Effects-Based Operations Models in War Games" (paper presented at the 8th International Command and Control Research and Technology Symposium, Washington DC, June 2003).
[18] See, for example, Food and Drug Administration, "An Overview of the CARVER Plus Shock Method for Food Sector Vulnerability Assessments" (U.S. Health and Human Services, July 2007).

The Meaning of Vulnerability in the Context of Critical Infrastructure Protection

William L. McGill and Bilal M. Ayyub

Abstract: This paper explores the concept of vulnerability in the context of critical infrastructure protection with the intent to establish an operational definition that provides a basis for meaningful measurement. Following a systematic consideration of the general elements of risk, it is observed that vulnerability as a notion provides a mapping between an initiating threat event and a resulting degree of loss. In light of homeland security problems, a mathematical expression for overall vulnerability is developed that divides the notion into two categories – *protection vulnerability* that focuses on those aspects of a system that influence the probability of damage or compromise given the occurrence of an initiating threat event (e.g., security system weaknesses, target accessibility, and fragility of targets), and *response vulnerability* that focuses on those aspects of a system that influence the probability of a specified degree of loss given damage or compromise (e.g., intrinsic resistance to loss and effectiveness of response and recovery capabilities). An operational definition for overall vulnerability is then proposed based on the initial observations and insights gained from developing the mathematical expression; that is, overall vulnerability describes the degree to which a system is susceptible to realizing a specified degree of loss following the occurrence of an initiating threat event. The paper concludes with a discussion of methods to assess the aggregate vulnerability of a system to a broader class of initiating threat types and offers a simple high-level procedure for implementing the developed ideas in an operational setting. It is emphasized throughout this paper that any statement about vulnerability must always be in reference to a specified degree of loss resulting from a specified initiating threat event; if either the initiating threat event (i.e., cause) or resulting degree of loss (i.e., consequence) is missing, any statement of vulnerability is meaningless.

1. INTRODUCTION

What does the term *vulnerability* mean in the context of critical infrastructure protection? Haimes (2004) defined the notion of vulnerability as follows: *vulnerability* is the manifestation of the inherent states of a system that renders it susceptible to damage or loss. A system is taken in the general sense to be a group of regular interacting and interconnected items that form a unified whole (Ayyub and Klir 2006). In a later publication, Haimes (2006) emphasized that vulnerability is a *multidimensional* concept best described by a suite of state variables that describe system weaknesses and how they interact to cause loss following a disruptive event. Numerous other researchers have explored the meaning of vulnerability in different contexts (e.g., Villagrán de León 2006; Hellström 2005; McEntire 2005; Agarwal et al. 2003; Paton and Johnson 2001; Weichselgartner 2001; Einarsson and Rausand 1998), and the general consensus is that any aspect of a system that weakens its ability to survive in a disruptive or hostile environment contributes to its overall vulnerability.

It is widely accepted that vulnerability is an important component of risk analysis (see Aven 2007; Haimes 2006; Pinto et al. 2003). As with vulnerability, *risk* is a multidimensional concept that describes the potential for loss associated with a disruptive event (Ayyub 2003) where, for a given event or scenario, the risk is the pairing of its probability of occurrence and the consequences given its occurrence (Kaplan and Garrick 1981). It can be inferred from the notions of vulnerability and risk that the weaknesses present in a system contribute to its potential for loss following an adverse event. Thus the quantification of risk necessarily requires meaningful ways to assess and measure vulnerability.

Despite this apparently obvious observation, numerous methods in current use within the critical infrastructure protection community do not assess vulnerability as a primary variable in its broadest sense, but rather capture elements of vulnerability implicitly through the assessment of other parameters. For example, in the Risk Analysis and Management for Critical Asset Protection (RAMCAP) methodology, the parameter "vulnerability" is equated to probability of adversary success, and other non-security related weaknesses are melded together under the heading of consequence assessment (Moore et al. 2007). The marginalization of vulnerability to a security issue is common in many other qualitative and quantitative security risk assessment methods. In contrast, many risk models for natural hazards identify vulnerability as the mapping from a state of damage to degree of loss, though in principle whether a system can be damaged in the first place is a question that should also fall under the heading of vulnerability assessment. Though different methodologies are permitted to slice and dice their expressions for risk in different ways that are all equally valid, they are consistent in their use of inconsistent and usually narrow definitions and measures for vulnerability.

Perhaps one reason for the apparent lack of an explicit definition for vulnerability in its broadest sense is the absence of an accepted understanding of what vulnerability tries to measure. Recently, Ayyub et al. (2007) developed an extensive expression for asset and portfolio risk in an all-hazards context from which, after careful observation of all risk contributors, emerged a mathematical expression for vulnerability that appears to capture the multidimensional essence of vulnerability. According to the authors, this expression explicitly identifies the major contributors to vulnerability in terms of interventions that limit the scope of outcomes between cause and consequence. This paper expands on the authors' observation and seeks to define an operational definition for vulnerability that facilitates its measurement in support of risk assessments for critical infrastructure protection.

To accomplish the objectives of this paper, section 2 provides an introduction to the basic philosophy of risk analysis and reasons how the notion of vulnerability fits within the overall picture of risk. Section 3 provides a discussion and develops a mathematical expression for overall vulnerability that captures what this term means in its broadest sense. Section 4 proposes an operational definition of vulnerability that supports structured vulnerability analysis, and offers a simplified expression and procedures for vulnerability assessment that could potentially improve how

vulnerability is interpreted and assessed in practical contexts. Section 5 concludes with a summary of the key points in this paper.

2. DEVELOPMENT OF THE RISK MODEL

The prototypical expression for risk in the homeland security context is traditionally written as:

$$Risk = Threat \times Vulnerability \times Consequence \quad (1)$$

where the total risk is the combination or Cartesian product of all relevant threat types, system weaknesses, and consequences resulting from when the damage-inducing mechanisms associated with the threats interact with the vulnerabilities. Risk, as Eq. 1 would suggest, tells a series of stories of all that could go wrong from initiating threat event to final outcome, where the heart of these stories, that is, the vulnerabilities, describe those weaknesses that must interact to make this scenario true. As a first step toward a quantitative expression for vulnerability, it would seem that vulnerability provides a mapping between the set of initiating threat events and the set of outcomes, such as is shown in Figure 1. In this view, any statement of vulnerability to a given initiating threat event must always be in reference to some degree of loss or adverse outcome, whether descriptive, qualitative, or quantitative in nature. Generic statements, such as "my vulnerability is high," are inherently ambiguous unless they are associated with some particular consequence, if even expressed on an arbitrarily constructed or vaguely defined scale (e.g., "my vulnerability to significant consequences is high").

In their seminal paper, Kaplan and Garrick (1981) put forth a quantitative definition of risk that is derived from the answers to three fundamental risk questions:

- What can go wrong?
- How likely is it to go wrong?
- What are the ensuing consequences?

The first question establishes a complete set of risk scenarios in narrative form and provides the basis for evaluation and quantification. As later elaborated by Kaplan et al. (2004), the level of specificity and detail chosen to articulate each scenario greatly affects how likelihood and consequence are assessed. Given a set of all possible scenarios of a specified type, highly detailed scenarios are larger in number and require more analytical effort to ascertain and assess, but provide a high resolution account and understanding of total risk. In contrast, less specific scenarios are fewer in number, but coincide with a greater uncertainty in the loss dimension to account for inexplicit variations in the nature and sequence of events between cause and consequence. For example, consider the very specific scenario "a medium-sized car bomb attack occurring at the federal building in downtown at 9:00am next Thursday." The details of this scenario permit a very good assessment of vulnerability to different degrees of loss given its occurrence, but completing the risk picture requires the decision maker to consider all variations that account for

different times, days, locations, delivery systems, and threat types. A less specific version of this scenario is "an explosive attack occurring in the region sometime in the next year" is inclusive of all specific scenarios of the previous example, but as such it is difficult make an all-encompassing assessment of overall vulnerability due to the wide variations in circumstances. Since vulnerability was defined to be a mapping from cause to consequence, it is thus important to construct scenarios that permit meaningful statements of vulnerability.

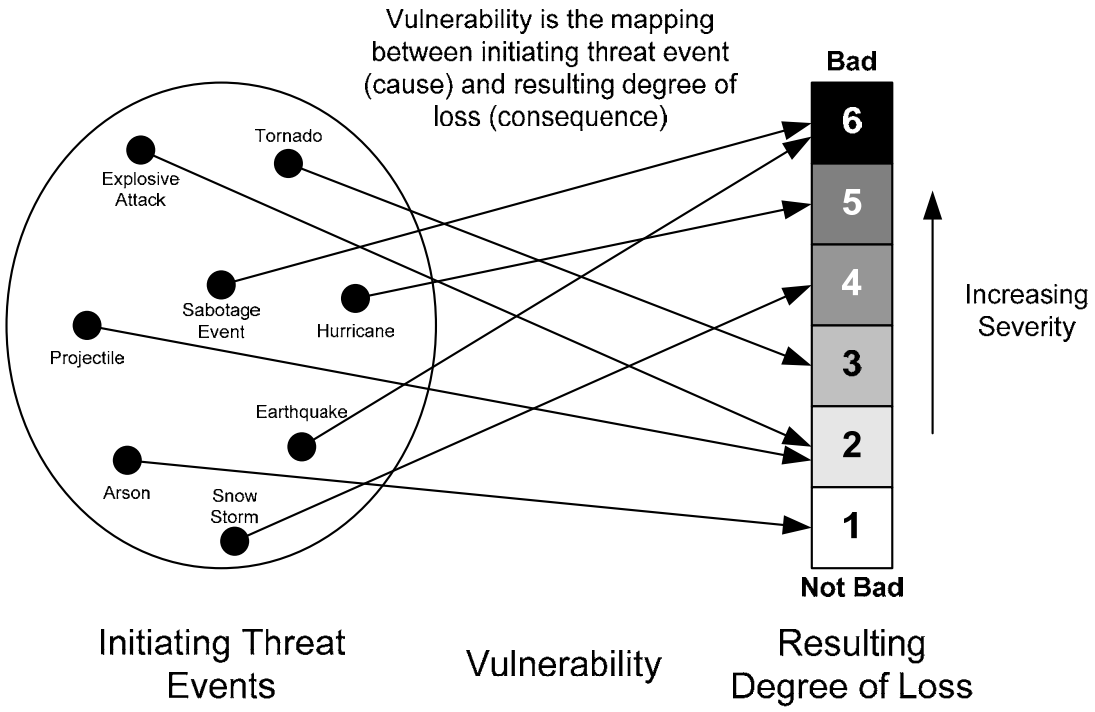


Figure 1. Vulnerability as the mapping between initiating threat events (i.e., cause) to resulting degree of loss (i.e., consequence)

Given a scenario, the risk, R_{ij}, can be expressed mathematically as the triplet of a scenario, e_i (i = 1, 2, . . . m), the probability of this scenario, p_{ij}, and consequence, c_j (j = 1, 2, . . . n), as follows:

$$R_{ij} = \langle e_i, p_{ij}, c_j \rangle \tag{2}$$

The equation above defines the risk triplet (Kaplan and Garrick 1981), where the scenario provides a narrative of a situation, the consequence is a valuation on the final outcome resulting from this situation, and the probability measures the likelihood that scenario e_i will lead to the consequence c_j. The total risk, R, is the set of all ordered triples, i.e., $R = \{R_{ij}\}$. The probability term, p_{ij}, in Eq. 2 is the joint probability of e_i and c_j, or:

$$p_{ij} = \Pr(e_i, c_j) = \Pr(c_j \mid e_i)\Pr(e_i) \quad (3)$$

where the operator Pr(.) defines the probability of the event contained in the parentheses. The manner in which the probabilities in Eq. 3 are assessed depends on how the scenarios E ($e_i \in E$) are articulated. As an example, if the scenarios specify in detail a sequence of events from initiating threat event to final outcome, then $\Pr(e_i)$ must consider the probability of each branch in an event tree defining the sequence, and $\Pr(c_j \mid e_i)$ defines a probability distribution over the space of consequences C ($c_j \subseteq C$, where c_j can be a range or interval over a finite set or single value among a discrete set) according to how the final outcome is valued by the decision maker in light of the residual uncertainties. In contrast, if the scenarios merely articulate an initiating threat event occurring at a specified location, then $\Pr(e_i)$ gives the probability of this initiating threat event occurring in a specified timeframe, and $\Pr(c_j \mid e_i)$ defines a probability distribution over C that accounts for the all the variations in subsequent events that lead to similar consequences. In this latter view, $\Pr(c_j \mid e_i)$ gives the probability that an initiating threat event, e_i, will lead to a consequence, c_j, or more generically, gives the probability that e_i will map to c_j. It can be said that this probability is a measure of vulnerability with respect to consequence c_j due to initiating threat event e_i, where $\Pr(c_j \mid e_i) = 1$ if e_i definitely leads to c_j, $\Pr(c_j \mid e_i) = 0$ if it is impossible for c_j to result from e_i, and $0 < \Pr(c_j \mid e_i) < 1$ according to how likely e_i will lead to c_j.

Building on the preceding discussion, the next section develops a mathematical expression for vulnerability based on the view that E defines a set of initiating threat events at a specified location where the probability, $\Pr(e_i)$, is the probability that the initiating threat event will occur at this location in a specified time period, and C defines a set of consequences (finite or continuous) that could result from these initiating threat events where the vulnerability term $\Pr(c_j \mid e_i)$ gives the probability that e_i will result in consequence c_j. For simplicity and ease of explanation, all probability distributions are represented in discrete form, though in practice many of these distributions may be continuous.

3. OVERALL VULNERABILITY ASSESSMENT

As described in section 2, the overall vulnerability of an individual decision maker to a given consequence, c_j, due to the occurrence of an initiating threat event, e_i, can be viewed as the probability that e_i leads to c_j, or $\Pr(c_j \mid e_i)$. Despite its apparent simplicity, there is richness to this expression that should not be underestimated. Given the occurrence of an initiating threat event, the assessment of overall vulnerability requires a thorough consideration of all intermediate interventions, whether active, passive, deliberate, or unintentional, between cause and consequence. In the case where there are no interventions, such as a naked man standing in a remote open field during a lightning storm, vulnerability assessment is easy: given that an intense bolt of lightning aims for this man, there is nothing to stop it from striking, nothing on the man to minimize its effects, nor are there first responders nearby to treat the man once zapped. Thus, the man's probability of realizing the consequence c_j = "immediate death" given that e_i = "the man is struck

by lightning" is high, perhaps around 0.9 (the residual probability of 0.1 is allocated toward the complementary event "not immediate death," which includes the consequences "delayed death" and "survival" with or without injury).

Most practical situations encountered by critical infrastructure protection practitioners are much more complicated than the "man in the field" scenario. Often, there are numerous interventions in place that seek to prevent a certain degree of loss following the occurrence of an initiating threat event, such as measures to harden critical assets against the damage-inducing effects of various threats, redundancies that limit cascading effects, response and recovery measures that seek to mitigate potential loss after an event, and measures to detect, respond to, and defeat adversaries in the case of malicious attacks. The event tree shown in Figure 2 illustrates a high-level sequence of interventions that seek to limit loss following an initiating threat event (shown for a malicious attack). A quick observation of this event tree suggests that the vulnerability to a given degree of loss with respect to an initiating threat event requires all intermediate interventions between cause and consequence to fail. In this context, the interventions behave in a manner consistent with a parallel systems reliability model (Modarres et al. 1999), where success of just one intervention prevents the specified degree of loss.

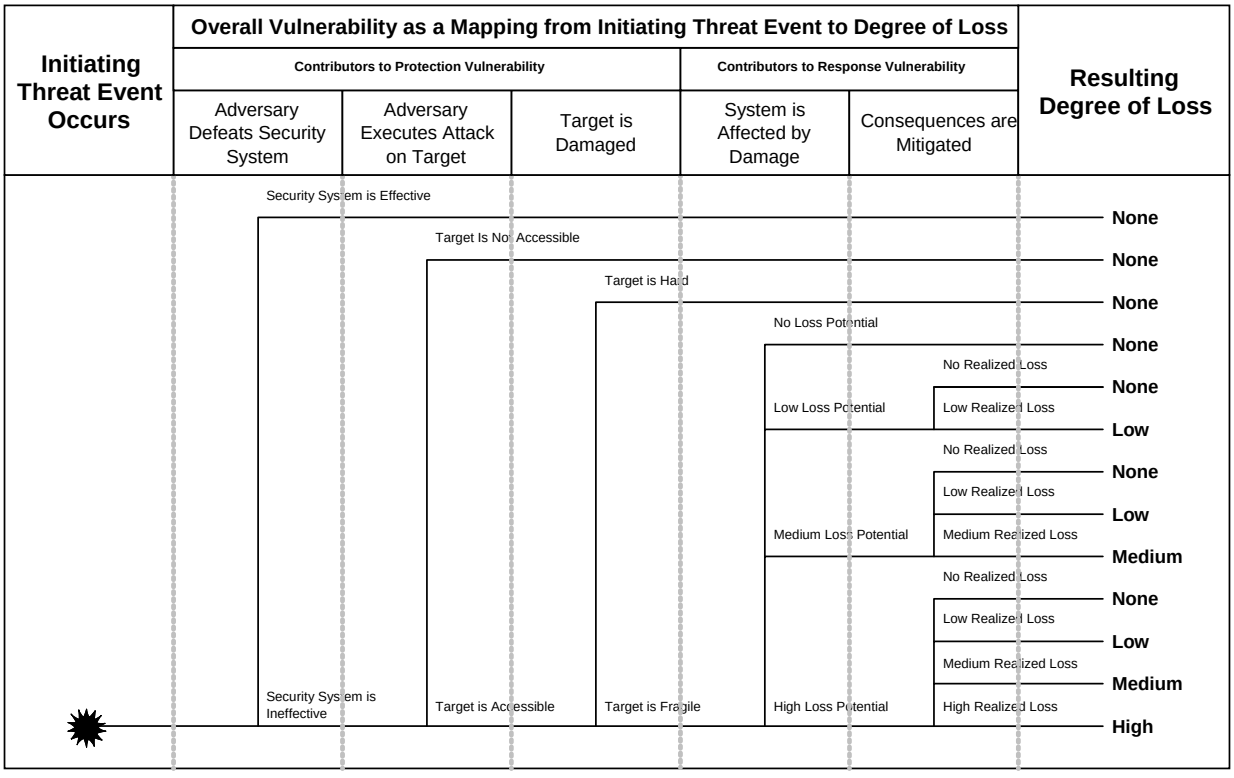


Figure 2. Sequence of interventions between initiating threat event to resulting degree of loss

Upon observation of Figure 2, one can divide the scope of overall vulnerability into two categories: *protection vulnerabilities* and *response vulnerabilities*. This division is similar to the categorical make-up of the DHS Target Capabilities List for dealing

with the effects of an initiating threat event (Department of Homeland Security 2006). Protection vulnerabilities include all weaknesses between the initiation of an adverse threat event and exposure of the targets to its damage-inducing mechanisms. Interventions to mitigate protection vulnerabilities include countermeasures that decrease the probability of adversary success and deny access to critical targets, and measures that improve hardness (or lessen the fragility) of potential targets with respect to the damage-inducing mechanisms of the threat. Response vulnerabilities include all deficiencies that serve to exacerbate the loss given damage of the targets. Interventions to mitigate response vulnerabilities include emergency response capabilities and measures that quickly reconstitute lifeline services following disruption. The following sections describe contributors to the overall vulnerability from each of these two categories, and develop mathematical expressions for protection vulnerability, response vulnerability, and overall vulnerability that facilitates its quantification for use in quantitative risk assessment.

3.1. Protection Vulnerability

The category *protection vulnerabilities* considers all contributors to overall vulnerability between the initiating threat event and damage of targets. That is, given the occurrence of an initiating threat event, protection vulnerability measures the probability of suffering a specified level of damage, whether in terms of damage or compromise of affected elements or size of an exposed human population. If damage cannot be reliably prevented following an initiating threat event, a target is vulnerable unless the system compensates with suitable strategies to control the ensuing losses. According to the event tree in Figure 2, a simple mathematical expression for protection vulnerability, $V_P(e_i, d_k)$, to a specified level of damage, $d_k \in D$, where D is a set of damage states, can be obtained as follows:

$$V_P(e_i, d_k) = \Pr(S \mid e_i)\Pr(K \mid S, e_i)\Pr(d_k \mid K, S, e_i) \tag{4}$$

where $\Pr(S \mid e_i)$ is the probability of adversary success given the occurrence of the initiating threat event, $\Pr(K \mid S,e_i)$ is the probability that the target will be exposed to the damage-inducing mechanisms of the threat given adversary success, and $\Pr(d_k \mid K,S,e_i)$ is the probability of damage given exposure of the target. According to this equation, an adversary must defeat a defender's protective measures, successfully execute the damage-inducing mechanisms of the attack, and then damage or compromise the target at a specified level, d_k, to achieve success. Equation 4 assumes that failure of the attacker to overcome the security system *OR* failure of the attacker to successfully execute his attack given the opportunity *OR* failure of the attack to cause damage d_k will result in no loss. Expressed in terms of favorable defender characteristics, Eq. 4 can be rewritten as:

$$V_P(e_i, d_k) = (1 - I_S(e_i))(1 - I_K(e_i))(1 - I_H(e_i, d_k)) \tag{5}$$

where $I_S(e_i) = 1 - \Pr(S \mid e_i)$ is the effectiveness of security system interventions with respect to initiating threat event e_i, $I_K(e_i) = 1 - \Pr(K \mid S,e_i)$ is the effectiveness of

interventions (intrinsic and extrinsic) that seek to deny execution of the attack against the specified target according to e_i given defeat of the defender force, and $I_H(e_i, d_k) = 1 - \Pr(d_k \mid K,S,e_i)$ measures the effectiveness of hardness interventions (intrinsic and extrinsic) of the target that minimize the ability to achieve damage state d_k given exposure to the damage-inducing mechanisms associated with e_i. Based on Eqs. 4 and 5, the three primary dimensions of protection vulnerability are *security system weaknesses*, *target accessibility*, and *fragility of target elements*. In the event of no security, complete target accessibility, and fragile targets, $I_S = I_K = I_H = 0$ and $V_P = 1$.

Note that for natural hazards, $I_S = 0$ and $I_K = 0$ since at the present time few feasible interventions are available to stop natural events once they are initiated. According to these simplifications, Eq. 5 can be rewritten for natural hazards as:

$$V_P(e_i, d_k) = (1 - I_H(e_i, d_k)) \tag{6}$$

A discussion of each dimension of protection vulnerability is provided in the following sections.

3.1.1. Security System Weaknesses

In order to minimize the probability of adversary success, the defender force must possess capabilities to effectively *detect*, *engage*, and *neutralize* determined adversaries considering a full spectrum of possible threat types and attack profiles. For a given malicious initiating threat event type (e.g., explosive attack), an attack profile is the pairing of a delivery mode (e.g., car) with a relevant intrusion path (e.g., via rear access road) (McGill et al. 2007). Security system effectiveness is based on the weakest link model – failure to detect, engage, or defeat a potential adversary maximizes the potential for adversary success (Hicks et al. 1987), such as would be the case in the absence of effective protective measures. Furthermore, as with most technological systems, the reliability of a security system, in general, is a function of hardware, software, and human elements, all of which are intertwined in complex ways. Security is thus a complex function of characteristics associated with the asset, defender, adversary, and the situation at hand (Manunta 1999).

3.1.1.1. Detection

Detection requires capabilities to *sense* the environment, *recognize* whether an attack is taking place, and *annunciate* these observations to a decision maker (e.g., watch guard) for action. For example, a security system comprised of a CCTV system equipped with intrusion detection software, trained watch personnel, and effective alert policies possesses the required elements of an effective detection capability. Similarly, a team of guards standing visual watch over a well-lit, security-friendly environment (Crowe 1991) also possesses the ability to sense, recognize, and annunciate attacks, even if not complemented by security technology.

Detection measures come in two types – static (demand-based) measures and active (time-dependent) measures. The performance of a static detection measure can be specified as the *probability of detection* that is a function of threat type and adversary capability. For example, the probability of detection for a trip wire depends on adversary awareness of this device and ability of the adversary to overcome this measure, whether deliberately or by accident. In contrast, a key measure of effectiveness of active detection measures could be the *mean time to detect* a given type of adversary and threat type; the value of this parameter is affected by the choice of detection elements and degree of implementation, to include policies, procedures, personnel training, and predictability.

3.1.1.2. Engagement

Engagement requires that the security system *delay* determined adversaries long enough for defenders to *respond* and *engage* the adversary. Delay measures include the distance between the boundary of the protected perimeter of an asset and the target element, as well as any physical barriers along the way such as gates, fences, moats, and bollards. A key measure of effectiveness for delay measures is *time to defeat*, which can be conservatively specified as a minimum value or characterized by the mean and coefficient of variation of a probability distribution. For example, the effectiveness of security doors is specified by the minimum time required to overcome the barrier to entry (e.g., a two-minute door). Response measures include suitable numbers and proper placement of guard forces or other response vehicles so as to minimize the *defender response time*. Engagement is achieved if the defender response time is sufficiently shorter than the time remaining for the adversary to execute an attack once detected.

3.1.1.3. Neutralization

Neutralization requires that defenders possess the ability to defeat determined adversaries once engaged. When viewed from a stress-strength point of view, neutralization occurs when the "strength" of the defender force exceeds the "stress" imposed on it by the adversaries. The strength of a defender force largely depends on the capabilities of security guards, which consider the size of the security force, available weapons, quality of training, and complex organizational factors such as morale (see Apostolakis 2004; Bunn 2004; Carroll 2004; Sagan 2004; Westrum 2004). Human reliability analysis (HRA) techniques can be used to estimate the probability of neutralization, such as by establishing a baseline probability of neutralization that is then modified according to the states of various *adversary performance influencing factors* or *performance shaping factors* such as skill, number of adversaries, and determination (see Chen and Mosleh 2007).

3.1.2. Target Accessibility

Given failure of the security system to successfully prevent the execution of an attack, adversary success still requires that the attacker successfully *accesses* and successfully *imparts its load* on the target. In many cases, access to the target is

assured in the absence or failure of a security system, thus leaving to chance whether the attack will go off as intended (e.g., a "dud" explosive). However, in some cases, such as a physically-enforced standoff attack, target access depends on the size of the target with respect to standoff distance. From a given distance, a small target is more difficult to hit than larger target. A cyber analog is access to an air-gapped SCADA system via the Internet: in this situation, access is *denied* since the chosen intrusion path cannot lead to the desired target.

3.1.3. Target Fragility

Fragility or *hardness* is a physical property of target elements that is tied to the degree of damage resulting from exposure to a hazard of specified intensity (Woo 1999). The performance of target elements under the load imparted by a given hazard or threat type is typically measured in terms of a *fragility curve* that specifies the probability of realizing a certain state of damage as a function of intensity (e.g., Ellingwood 2001). For populations of humans exposed to biological or chemical hazards, such fragility curves are called dose-response curves (Kowalski 2002). An element is said to be "hard" with respect to a given threat type if the probability of damage is low relative to the range of possible intensities. Conversely, an asset is said to be "fragile" if small intensities lead to significant damage. The hardness of an asset or system element can only be improved through engineering (e.g., blast retrofitting).

3.2. Response Vulnerability

The category *response vulnerabilities* consists of all contributors to vulnerability that influence the degree of loss that would be realized given that specified initiating threat event e_i resulted in damage state d_k. That is, response vulnerability measures the probability of a specified consequence or outcome associated with a given damage state. If loss cannot be effectively controlled, then the asset is vulnerable unless this deficiency is compensated for by effective protective measures that minimize probability of adversary success. According to the event tree in Figure 2, a simple mathematical expression for response vulnerability, $V_R(c_j, d_k)$, for a given degree of loss, c_j, resulting from damage state d_k can be expressed as:

$$V_R(c, d_k) = \sum_m \Pr(c \mid c_{P,m}) \Pr(c_{P,m} \mid d_k) \tag{7}$$

where $\Pr(c_{P,m} \mid d_k)$ is the probability that a loss, $c_{P,m}$, could result from damage state d_k (which is a measure of the intrinsic resistance of the target systems to loss), $\Pr(c_j \mid c_{P,m})$ is the probability that the actual loss is c_j in light of the effectiveness of response and recovery capabilities given that the unmitigated loss was $c_{P,m}$, and the summation is taken over all m states of unmitigated loss. Eq. 7 assumes that the response vulnerabilities are assessed independently of the scenario that initiated damage state d_k, which may be true for the "crisp" consequence dimensions such as direct economic damage and number of fatalities, but less true for the "softer," less

ascertainable dimensions such as psychological impact. Expressed in terms of favorable defender characteristics, Eq. 7 can be rewritten as:

$$V_R(c_j, d_k) = \sum_m \left(1 - I_R(c_j, c_{P,m})\right)\left(1 - I_I(c_{P,m}, d_k)\right) \quad (8)$$

Based on Eq. 8, the two dimensions of response vulnerability are *intrinsic susceptibility of a system to loss following damage* and the *effectiveness of response and recovery capabilities*.

3.2.1. Intrinsic Vulnerability

Given some level of damage associated with a target element, the ensuing loss depends on the *intrinsic vulnerability* to loss that accounts for the value of the target, and the physical, geographical, cyber, and logical connectedness (Rinaldi et al. 2001) of the target element with respect to a larger system defined by the needs and concerns of a specific decision maker, such as an asset owner, regulating agency, or regional policymaker. For example, damage to a redundant component of a power plant might be significant from an asset owner's perspective since the component must be repaired or replaced, but may be inconsequential for those responsible for the regional energy grid if the system is able to meet consumer demands. Intrinsic vulnerability is measured as the probability of realizing a specified degree of loss following damage in the absence of post-event mitigation measures, and as such depends on the definition of the system and its interdependencies, the context in which it is viewed, and consequence dimensions considered.

3.2.2. Response and Recovery

The loss following the occurrence of an adverse event can be tempered with measures to *respond to* and *recover from* an event. Response measures seek to quickly contain immediate loss, such as responding to a mass casualty or mass exposure incident with effective triage and treatment capabilities. For example, measures to enhance disaster preparedness fall under this category (e.g., community planning, establishing evacuation routes) (McGill 1957). Recovery measures seek to restore an affected asset or system to its pre-incident condition, such as by reducing the duration of accumulating losses. The effectiveness of response and recovery is measured as probability of realizing a specified degree of loss given a prescribed loss potential in the mitigated state.

3.3. Overall Vulnerability

Given the expressions for protection vulnerability, V_P, and response vulnerability, V_R, the overall vulnerability, V_T, of a target to a given degree of loss, L, resulting from initiating threat event e_i can be expressed as:

$$V_T(c_j, e_i) = \sum_k V_P(e_i, d_k) V_R(c_j, d_k) \quad (9)$$

Using the expressions for V_P in Eq. 5 and V_R in Eq. 8, overall vulnerability can be expressed in expanded form as:

$$V_T(c_j, e_i) = \sum_k \sum_m (1 - I_S(e_i))(1 - I_K(e_i))(1 - I_H(e_i, d_k))(1 - I_R(c_j, c_{P,m}))(1 - I_I(c_{P,m}, d_k)) \quad (10)$$

where the summation is taken over all possible damage states *k*. Equation 10 permits statements about the vulnerability of a system to a specified degree of loss resulting from a specified initiating threat event. For example, a team of analysts and engineers can employ Eq. 10 to assess the overall vulnerability of a company to 100 or more fatalities following a truck bomb attack in an underground parking structure. To make statements about overall vulnerability of the company to 100 or more fatalities resulting from an explosive or malicious attack *in general* (considering all delivery modes, targets, and intrusion paths) requires an aggregation of the overall vulnerability for each individual attack profile and initiating threat event considered.

3.4. Aggregate Vulnerability

Given a set of initiating threat events, e_i, belonging to a class of threat types, E ($e_i \in E$), (such as explosive attacks, malicious attacks, or natural hazards), the aggregate vulnerability, V_A, of the system to a degree of loss, c_j, can be obtained as:

$$V_A(c_j \mid E) = \sum_i V_T(c_j, e_i) \Pr(e_i \mid E) \quad (11)$$

where $\Pr(e_i \mid E)$ is the conditional probability of e_i given the occurrence of E, and the summation is taken over all initiating threat events i belonging to E. In the case of natural hazard events, such as tropical cyclones, application of Eq. 11 is relatively straightforward, where E = {Tropical Depression, Tropical Storm, Cat 1, Cat 2, . . . Cat 5} if one chooses to partition the set of initiating threat events according to the Saffir-Simpson scale (Woo 1999). More complicated are malicious attacks, where the probability of an initiating threat event depends on the relative attractiveness of the scenario with respect to other options considered by the adversary. In general, malicious threats are intelligent, innovative, and adaptive, and assessing the probability of a malicious initiating threat event thus requires consideration of intents, motivations, creativity, capabilities, and overall awareness of potential targets, threat types, and scenarios.

One approach to assessing the relative probability of malicious initiating threat events is the proportional attractiveness method initially described by McGill et al. (2007), where it is assumed that the probability of attack for a given initiating threat event is proportional to the expected utility of e_i, $U_P(e_i)$, as perceived by the adversary weighted by the visibility of the target or threat type, $\Pr(P \mid e_i)$, or:

$$\Pr(e_i \mid E) = \frac{\Pr(P \mid e_i) U_P(e_i)}{\sum_j \Pr(P \mid e_j) U_P(e_j)} \tag{12}$$

where the summation in the denominator is taken over all initiating threat events belonging to *E*. According to Eq. 12, any change in the perceived utility of an initiating threat event, such as would be due to the implementation of new interventions that limit loss or probability of adversary success, will update (perhaps decrease) the probability of occurrence with respect to the other initiating threat events considered. The perceived utility term, U_P, in Eq. 12 can be expressed as:

$$U_P(e_i) = \max\left(G_i^* S_i^* - L_i^*(1 - S_i^*) - C_i^*, 0\right) \tag{13}$$

where G_i^* is the perceived benefit or gain from success, L_i^* is the perceived loss from failure, S_i^* is the perceived probability of success, and C_i^* is the perceived cost of resources to plan and execute (the asterisk is used to denote variables dependent on adversary perceptions). The max function in Eq. 13 is used to exclude those initiating threat events with a negative perceived expected utility.

According to the forms of Eqs. 12 and 13, the conditional probability of an initiating threat event depends on an adversary's awareness of potential targets and perceptions of gain, loss, probability of success, and cost. In light of the expression for aggregate vulnerability in Eq. 11, the aggregate vulnerability for malicious attacks depends on adversary awareness and perceptions, which can be influenced by interventions that limit visibility and enhance deterrence. These considerations in the context of aggregate vulnerability are described in the following sections.

3.4.1. Visibility

As can be seen from Eq. 12, the *visibility* of asset or system elements and intrusion paths has a significant effect on aggregate vulnerability. If an element or intrusion path is not visible to an adversary, then the associated initiating threat events would not be considered. Visibility depends on the amount of information available to the adversary to assist in attack planning, such as information gained through surveillance and reconnaissance or from open sources (Baker et al. 2004; Pluchinsky 2002). Strategies to minimize visibility serve to decrease aggregate vulnerability; however, difficulties in assessing what is truly visible to a potential adversary make this contributor hard to measure. A conservative approach to vulnerability assessment is to assume all assets, elements, and intrusion paths are visible to the adversary (i.e., probability of adversary awareness is one); any additional measures to limit visibility provide a bonus, though largely unassessed, improvement to aggregate vulnerability.

3.4.2. Perceived Attractiveness

As noted by Fuqua and Wilson (1977), *deterrence* affects the psyche of the adversary, and thus has influence only over the choice of whether to attack and which attack profile to choose. In general, all visible interventions and countermeasures have some deterrence value. The addition of deterrence measures designed solely for influencing adversary perceptions has the positive effect of moving adversary attention away from less protected elements and intrusion paths, and thus decreases aggregate vulnerability. While having no bearing on the actual performance of an asset under the stress imposed by an adversary, measures such as fake cameras, decoy guards, signage, and mock targets serve to decrease vulnerability by creating the appearance of tight security or by creating undesirable attack options. As with visibility, however, the difficulty in assessing the perceptions of potential adversaries is difficult at best, and thus aggregate vulnerability should be conservatively assessed under the assumption of perfect adversary knowledge of the all critical elements, their loss potential, and the existence and effectiveness of interventions (i.e., the "mirror-imaging" assumption per McGill et al. (2007)).

3.5. Observations on Aggregate Vulnerability

For classes of natural hazards events where, in general, there is an inverse relationship between relative probability of occurrence and intensity, the higher vulnerability to loss at higher intensities is compensated by the fact that the probability of the event's occurrence is smaller. From Eq. 11, it can be observed from the inverse relationship between probability and intensity that $V_T(c_j \mid E) \geq V_A(c_j, e_i)$ for all $e_i \in E$ since $V_A(c_j, e_2) \geq V_A(c_j, e_1)$ when $\Pr(e_2 \mid E) \leq \Pr(e_1 \mid E)$. That is, for natural hazards, the aggregate vulnerability of a system to a specified degree of loss for a given class of initiating threat events is always greater than or equal to the overall vulnerability to the same degree of loss resulting from a single initiating threat event from this class.

This same argument does not necessarily hold for classes of malicious initiating threat events. In particular, according to the weighted attractiveness method for assessing the probability of an initiating threat event, the total mass of probability is biased toward those initiating threat events that are more attractive to the adversary from the standpoint of perceived expected utility. Under the conservative "mirror-imaging" assumption that assumes the adversary has perfect knowledge of system vulnerability, there exists a direct relationship between overall vulnerability and relative probability of occurrence for a given initiating threat event. That is, the more vulnerable a system is to a given initiating threat, the more likely the initiating threat event is to occur. Though in most circumstances this assumption is conservative, the fact that knowledge of adversary perceptions, motivations, capabilities, etc. is inherently limited justifies its use from a risk practitioner's point of view. Unfortunately, the implications of this assumption is that a high overall vulnerability to loss from just one initiating threat event among a class of events dominates the aggregate vulnerability, whereas for natural hazards this would not necessarily be the case.

4. TOWARD AN OPERATIONAL DEFINITION OF OVERALL VULNERABILITY

4.1. Vulnerability as a Notion

The purpose of the discussion to this point was to provide the background needed to establish an operational definition for the term *overall vulnerability* by parsing out all contributors to vulnerability from a developed expression for risk in the context of critical infrastructure protection. An operational definition for a concept or idea is one that facilitates the construction of meaningful measures of magnitude. Based on this discussion, the following operational definition of vulnerability is proposed:

> **Definition:** *Overall vulnerability* is a multidimensional property of a system that describes the degree to which it is susceptible to realizing a specified degree of loss following the occurrence of an initiating threat event. Overall vulnerability consists of both protection vulnerabilities and response vulnerabilities. *Protection vulnerability* describes the probability of realizing damage following an initiating threat event, and considers the fragility of critical elements, target accessibility, and security system weaknesses. *Response vulnerability* describes the probability of realizing loss given damage considering the intrinsic susceptibilities of the target system to loss and the availability of response and recovery measures. *Aggregate vulnerability* is the sum of the overall vulnerability for a variety of alternative initiating threat events weighted according to their relative probability of occurrence which, in the case of malicious initiating threat events, can be influenced by visibility and attractiveness.

According to this definition, vulnerability can be alleviated through the implementation of suitable measures and interventions that minimize visibility, attractiveness, probability of adversary success, probability of damage given success, and susceptibility to loss given damage.

4.2. Vulnerability as a Measure

As developed in section 3, the overall vulnerability, $V_T(c_j, e_i)$, of a system to a specified degree of loss, c_j, resulting from a specified initiating threat event, e_i, is equal to the probability of this degree of loss given the occurrence of this initiating threat event, or:

$$V_T\left(c_j, e_i\right) = \Pr\left(c_j \mid e_i\right) \tag{14}$$

In light of the interventions between cause or initiating threat event e_i and consequence c_j, such as protective measures and response and recovery measures, Eq. 10 provides an expanded expression for vulnerability considering multiple damage states.

For the simplified case of one adverse damage state, *D* (such as would correspond to "unacceptable damage"), and one state of loss, *C* (such as would correspond to "unacceptable loss"), the expressions for protection vulnerability, V_P, response vulnerability, V_R, and overall vulnerability, V_T, with respect to initiating threat event e_i can be restated in simplified form as:

$$V_P(e_i, D) = (1 - I_S(e_i))(1 - I_K(e_i))(1 - I_H(e_i, D)), \tag{15}$$

$$V_R(C, D) = (1 - I_R(C, C))(1 - I_I(C, D)), \text{ and} \tag{16}$$

$$\begin{aligned} V_T(C, e_i) &= V_P(e_i, D) V_R(C, D) \\ &= (1 - I_S)(1 - I_K)(1 - I_H)(1 - I_R)(1 - I_I) \end{aligned} \tag{17}$$

Observe that under the assumption of single states of damage and loss, the expression for overall vulnerability for a given initiating threat event assumes the form of a parallel system model in terms of interventions. That is, the presence of a single perfectly effective intervention (i.e., equal to one) renders the entire system invulnerable to unacceptable loss. In contrast, all interventions must be absent (i.e., equal to zero) to render the system completely vulnerable. The form of Eq. 17 suggests that the absence of any given intervention (e.g., no security system) can be compensated for by the implementation of interventions in other areas (e.g., hardened assets).

In terms of the simplified expression for overall vulnerability in Eq. 17, aggregate vulnerability assuming single states of damage and loss can be written as:

$$V_A(C \mid E) = \sum_i V_T(C, e_i) \Pr(e_i \mid E) \tag{18}$$

where the summation is taken over all initiating threat events *i* belonging to *E*. Equation 18 suggests that the magnitude of the aggregate vulnerability to loss *C* depends on both the overall vulnerability to specific initiating threat event *E* and its relative probability of occurrence. As described in section 3.4., for classes of malicious initiating threat events, the aggregate vulnerability term in Eq. 18 is directly related to overall vulnerability, and thus Eq. 18 serves to bias aggregate vulnerability towards those initiating threat events having a higher overall vulnerability. In contrast, for classes of natural hazard events, it is generally assumed that the probability of an initiating threat event is inversely related to intensity, and thus inversely related to overall vulnerability. That is, unlike for malicious events, the high overall vulnerability to high intensity natural hazard events is compensated for by a decreased probability of occurrence.

4.3. Making Statements about Overall Vulnerability

As often emphasized throughout this paper, any statement about the overall vulnerability of a system must be in reference to a clearly defined initiating threat

event and some degree of loss, whether this degree of loss has a clear extension with clear intension (e.g., a specific value such as $10,000), clear extension with vague intension (e.g., a range or interval of values, such as >100 fatalities), or clear intension with vague extension (e.g., a linguistic value for loss such as "high"). If either the initiating threat event (i.e., cause) or the degree of loss (i.e., consequence) is absent, any statement about vulnerability is meaningless. This can also be seen from the mathematical expressions for vulnerability developed in section 3 and restated early in section 4 – no assessment of vulnerability can be made without values for the input arguments e_i and c_j. Again, it is meaningless to say "my vulnerability is high" unless this statement is further qualified by a degree of loss and an initiating threat event (e.g., "my vulnerability to death from a lightning strike is high").

Furthermore, the mathematical expressions for overall vulnerability and aggregate vulnerability developed in previous sections do not necessarily insist on the use of probabilities or numbers for the model parameters. In the most general sense, these expressions rather only insist on the logical relationship between the interventions assessed as inputs and the overall vulnerability as an output (e.g., the "parallel systems" structure under the assumptions of single states of damage and loss). Thus, given a proper question about vulnerability that includes both an initiating threat event and consequence of concern (e.g., "what is my overall vulnerability to death if I am struck by lightning?"), it is admissible to make linguistic assessments regarding the effectiveness of interventions and overall vulnerability (e.g., "high," "medium," and "low") so long as the underlying structural relationship between the inputs and output remains intact.

4.4. Assessing Overall Vulnerability

The expression for overall vulnerability in Eq. 14 not only provides a basis for establishing a measure for vulnerability, but the simplified expressions for overall vulnerability in Eq. 17 and aggregate vulnerability in Eq. 18 provide a basis for assessing vulnerability. A high-level process for assessing the overall vulnerability of an asset or system is outlined in Figure 3. According to Eq. 18, the assessment of aggregate vulnerability requires a thorough consideration of all initiating threat events belonging to a given class of events, such as natural hazards or malicious attacks. For example, if explosive threats to a downtown office building are of concern, an exhaustive set of disjoint initiating threat events that consider variations in delivery systems (e.g., truck, hand emplaced, or aerial vehicle) and intrusion paths (e.g., via rear access road, via main entrance, or via air) against key asset elements (e.g., people, main building, or backup generator) would be considered. McGill et al. (2007) provides additional guidance on constructing attack profiles for a given threat type that are relevant to an asset or system. For classes of natural hazard events, one could partition the set of initiating threat events according to established intensity scales, such as the Saffir-Simpson scale for tropical cyclones, Richter scale for earthquakes, or Fujita scale for tornadoes.

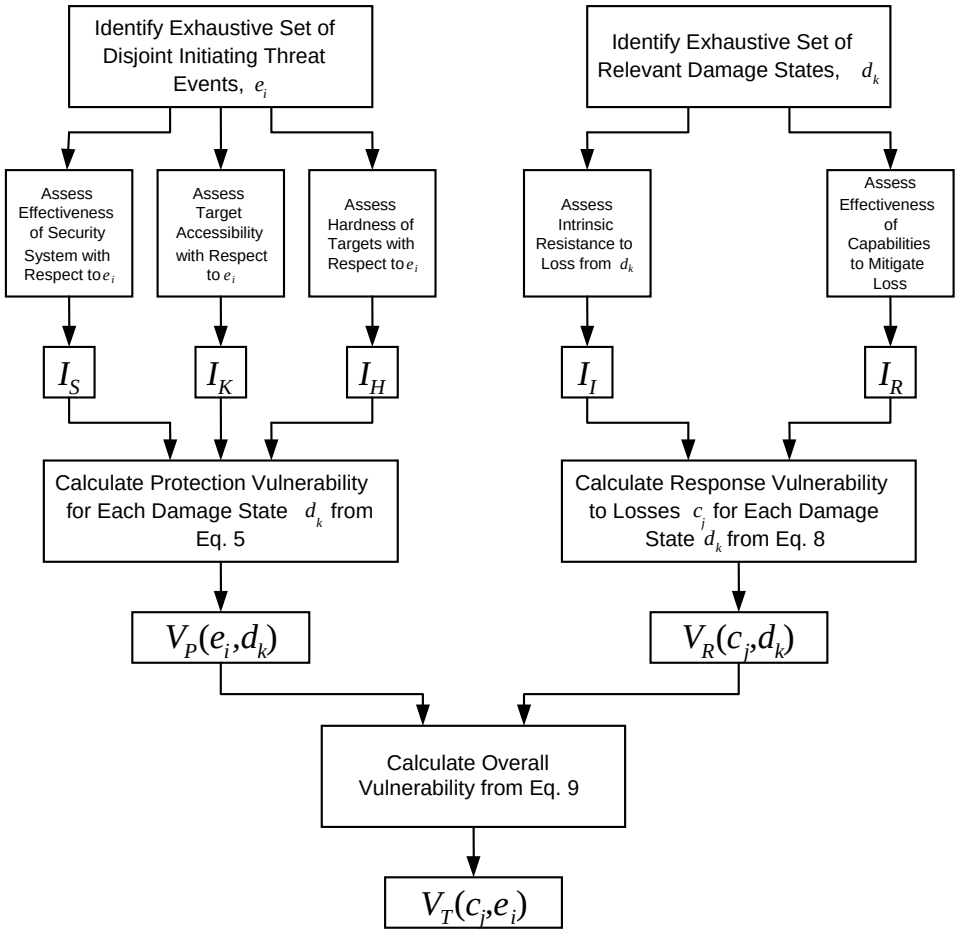


Figure 3. Process for overall vulnerability assessment

Given a complete set of initiating threat events, the overall vulnerability to loss resulting from each initiating threat event is assessed by considering the effectiveness of existing interventions for reducing protection vulnerability and response vulnerability in light of the intensity of the damage-inducing mechanisms associated with the threat. More specifically, the effectiveness of interventions (both extrinsic and intrinsic) to improve security (I_S), decrease target accessibility (I_K), and enhance target hardness (I_H) are assessed with respect to each initiating threat event to determine the corresponding probability of damage. Independent of an initiating threat event, the effectiveness of interventions to improve intrinsic resistance to loss (I_I) and enhance response and recovery capabilities (I_R) is considered to determine the probability of realizing a specified degree of loss given damage. That is, the assessment of protection vulnerability considering I_S, I_K, and I_H requires the analyst to specify a set of damage states, and the assessment of response vulnerability considering I_I and I_R requires the analyst to specify a set of loss levels or ranges of interest. If it can be assumed that loss is tied strictly to damage, then response vulnerability can be assessed independently of protection vulnerability.

5. CONCLUSIONS

Acceptable results from any type of analysis must follow from an acceptable process (Reid 1992). Accordingly, an acceptable process for vulnerability assessment requires an acceptable operational definition for vulnerability in order to make sense of information gathered during a vulnerability assessment and to provide meaningful measures of magnitude. This paper provided such an operational definition for overall vulnerability that emerged from the systematic consideration of the elements of risk, which then provided a basis for establishing a mathematical expression for overall vulnerability to a specified degree of loss due to a specified initiating threat event. Moreover, this paper emphasized that:

- Overall vulnerability is a multidimensional concept that describes the degree to which a system is susceptible to a specified degree of loss resulting from a specified initiating threat event. That is, overall vulnerability provides a mapping between initiating threat events and the resulting consequences, where the strength of this mapping provides a measure of vulnerability in terms of joint probability.
- Overall vulnerability can be divided into two categories – protection vulnerabilities and response vulnerabilities.
    - Protection vulnerabilities influence the probability of damage for different damage states for a given initiating threat event. Interventions that seek to minimize the probability of damage include protective measures, measures that reduce target accessibility, and measures that improve the hardness of target elements.
    - Response vulnerabilities influence the probability of a specified type or degree of loss following damage, and are largely independent of the nature of the initiating threat event. Interventions that seek to minimize the probability of loss include measures that improve the intrinsic resistance of the affected systems to loss and measures that enhance response and recovery capabilities.
- Statements of overall vulnerability must always be in relation to a specified degree of loss resulting from a clearly articulated initiating threat event. If either the initiating threat event (i.e., cause) or ensuing degree of loss (i.e., consequence) are missing from a statement about overall vulnerability, that statement is then meaningless.
- Broader statements of aggregate vulnerability to a specified class of initiating threat events (e.g., malicious attacks or natural hazards) are obtained as the sum of the overall vulnerability to each individual threat event weighted by its probability of occurrence relative to other initiating threat events in the same class.
    - For natural hazards, it can be reasonably assumed that the probability of an initiating threat event is inversely related to its intensity. Therefore, the increased overall vulnerability to high intensity events is compensated by a decreased probability for that event, and thus the aggregate vulnerability is biased toward low intensity events.

  - For malicious attacks, the weighted attractiveness method assumes that the probability of an initiating threat event is directly related to its intensity, and thus probability increases with increasing overall vulnerability for a given degree of loss. In this case, the aggregate vulnerability is biased toward those events tied to or associated with the highest overall vulnerability. Despite this, there exist options to decrease this relationship between vulnerability and probability of event, such as through measures that decrease visibility of the target, its assets, and intrusion paths and measures that increase the deterrence or decrease the attractiveness of the alternative initiating threat events.
- If one assumes a single damage state (e.g., "unacceptable damage") and a single state of loss (e.g., "unacceptable loss"), the expression for overall vulnerability with respect to a given initiating threat event assumes the form of a parallel system model. That is, the existence of just one perfectly effective intervention renders a system invulnerable, whereas all interventions must be ineffective for the system to be completely vulnerable.

It is hoped that this paper will inspire critical infrastructure protection researchers and practitioners to adopt the proposed definition and expressions for vulnerability as the basis for future vulnerability studies.

William L. McGill, P.E., C.R.E., has extensive experience applying risk analysis to homeland security, defense, and engineering problems. He has authored several academic publications on the topic of risk and homeland security, and is currently finishing his doctorate degree at the University of Maryland on the topic of risk methods for critical asset protection. In 2003, Mr. McGill served a one-year appointment as the American Society of Mechanical Engineers (ASME) Fellow to the Department of Homeland Security's Information Analysis and Infrastructure Protection Directorate, where he supported the initial efforts to develop DHS-risk analysis processes. More recently, Mr. McGill has served on DHS-sponsored expert panels on risk assessment methodologies.

Bilal M. Ayyub, Ph.D., P.E., is a Professor of Civil and Environmental Engineering and the Director of the Center for Technology and Systems Management at the University of Maryland (College Park). He is the president of BMA Engineering, Inc. Dr. Ayyub has an extensive background in uncertainty modeling and analysis, risk-based analysis and design, simulation, and marine systems. He has completed several research projects that were funded by the National Science Foundation, Air Force, Coast Guard, Army Corps of Engineers, Department of Homeland Security, the Maryland State Highway Administration, the American Society of Mechanical Engineers, and several engineering companies. Dr. Ayyub is a fellow of ASCE, ASME and SNAME, and has served the professional community in various capacities through societies that include ASNE, ASCE, ASME, SNAME, IEEE-CS, and NAFIPS. He is the author and co-author of more than 450 publications in journals and conference proceedings, and reports. His publications include several textbooks. Dr. Ayyub is a multiple recipient of the ASNE "Jimmie" Hamilton Award for the best papers in the Naval Engineers Journal in 1985, 1992, 2000 and 2003. Also, he received the ASCE "Outstanding Research Oriented Paper" in the Journal of Water Resources Planning and Management for 1987, the ASCE Edmund Friedman Award in 1989, the ASCE Walter Huber Research Prize in 1997, and the K. S. Fu Award of NAFIPS in 1995.

ACKNOWLEDGMENTS

Support for this work was provided in part by the Maryland Emergency Management Agency under a grant to the Center for Technology and Systems Management at the University of Maryland, College Park. For their helpful comments and discussions, the authors thank colleagues at the Argonne National Laboratory, Los Alamos National Laboratory, and the Department of Homeland Security, in particular Dr. Jim Peerenboom, Ms. Melanie Tompkins, Dr. Earl "Rusty" Lee, Dr. Alexia Brunet, Ms. Rebecca Haffenden, and Mr. Donald Neale. Moreover, the authors would like to acknowledge the support of several undergraduate researchers at the University of Maryland, notably Mr. Josh Hollands, Mr. Brett Kuklewicz, and Mr. Chris Watson.

REFERENCES

Apostolakis, G. E. (2004). "Redundancy and Nuclear Security." Risk Analysis, Vol. 24, No. 4, pp. 947-948. doi:10.1111/j.0272-4332.2004.00496.x

Argarwal, J., Blockley, D., and Woodman, D. (2003). "Vulnerability of Structural Systems." Structural Safety, Vol. 25, No. 3, pp. 263-286. doi:10.1016/S0167-4730(02)00068-1.

Aven, T. (2007). "A Unified Framework for Risk and Vulnerability Analysis Covering Both Safety and Security." Vol. 92, No. 6, pp. 745-754. doi:10.1016/j.ress.2006.03.008.

Ayyub, B. M., McGill, W. L., and Kaminskiy, M. P. (2007). "Critical Asset and Portfolio Risk Analysis for Homeland Security: An All-Hazards Approach." Risk Analysis, In press.

Baker, J. C., Lachman, B. E., Frelinger, D. R., O'Connell, K. M., Hou, A. C., Tseng, M. S., Orletsky, D., and Yost, C. (2004). Mapping the Risks: Assessing the Homeland Security Implications of Publicly Available Geospatial Information, RAND Document MG-142-NGA. ISBN:0833035479.

Broder, J. F. (1984). Risk Analysis and the Security Survey. Massachusetts: Butterworth Publishers. ISBN:0750694300.

Bunn, M. (2004). "Thinking About How Many Guards Will Do the Job." Risk Analysis, Vol. 24, No. 4, pp. 949-954. doi:10.1111/j.0272-4332.2004.00497.x

Carroll, J. S. (2004). "Redundancy as a Design Principle and an Operating Principle." Risk Analysis, Vol. 24, No. 4, pp. 955-957. doi:10.1111/j.0272-4332.2004.00498.x

Chen, Y. H. J., and Mosleh, A. (2007). "Cognitive Modeling and Dynamic Probabilistic Simulation of Operating Crew Response to Complex System Accidents. Part 2: IDAC Performance Influencing Factors Model." Reliability Engineering & System Safety, Vol. 92, No. 8, pp. 1014-1040. doi:10.1016/j.ress.2006.05.010

Crowe, T. D. (1991). Crime Prevention Through Environmental Design. Butterworth-Heinemann. ISBN:0750690585.

Dessent, G. H. (1987). "Prison Perimeter Cost Effectiveness." Journal of the Operational Research Society, Vol. 38, No. 10, pp. 975-980.

Department of Homeland Security (2006). Target Capabilities List version 2.0.

Einarsson, S., and Rausand, M. (1998). "An Approach to Vulnerability Analysis of Complex Industrial Systems." Risk Analysis, Vol. 18, No. 5, pp. 535-546. doi:10.1111/j.1539-6924.1998.tb00367.x.

Ellingwood, B. (2001). "Earthquake Risk Assessment of Building Structures." Reliability Engineering & System Safety, Vol. 74, No. 3, pp. 251-262. doi:10.1016/S0951-8320(01)00105-3.

Fuqua, P., & Wilson, J. V. (1977). Terrorism: The Executive's Guide to Survival. Texas: Gulf Publishing Company. ISBN:0872018210.

Gheorghe, A. V., and Vamanu, D. V. (2004). "Towards QVA-Quantitative Vulnerability Assessment: A Generic Practical Model." Journal of Risk Research, Vol. 7, No. 6, pp. 613-628. doi: 0.1080/1366987042000192219.

Gibson, S. D. (2003). "The Case for 'Risk Awareness'." Security Journal, Vol. 16, No. 3, pp. 55-64. doi:10.5555/sj.2003.16.3.55.

Grabo, C. M. (2004). Anticipating Surprise: Analysis for Strategic Warning. University Press of America. ISBN:0761829520.

Haimes, Y. Y. (2004). Risk Modeling, Assessment, and Management. 2nd Ed. Wiley, NY. ISBN:0471480487.

Haimes, Y. Y. (2006). "On the Definition of Vulnerabilities in Measuring Risks to Infrastructures." Risk Analysis, Vol. 26, No. 2, pp. 293-296. doi: 10.1111/j.1539-6924.2006.00755.x.

Hellström, T. (2005). "A Decision Model for Involvement in Vulnerability Reduction." Disaster Prevention and Management, Vol. 14, No. 2, pp. 196-205. doi:10.1108/09653560510595191.

Hicks, M. J., Snell, M. S., Sandoval, J. S., & Potter, C. S. (1999). "Physical Protection Systems – Cost and Performance Analysis: A Case Study." IEEE AES Systems Magazine, April.

Hoffman, B. (1998). Inside Terrorism. New York: Columbia University Press. ISBN:0231114699.

Kaplan, S., and Garrick, B. J. (1981). "On the Quantitative Definition of Risk." Risk Analysis, Vol. 1, No. 1, pp. 11-27. doi:10.1111/j.1539-6924.1981.tb01350.x.

Kowalski, W. J. (2002). "Immune Building Systems Technology." McGraw-Hill. ISBN:0071402462.

Manunta, G. (1999). "What is Security?" Security Journal, Vol. 12, No. 3, pp. 57-66. doi:10.5555/sj.1999.12.3.57.

Martz, H. F., and Johnson, M. E. (1987). "Risk Analysis of Terrorist Attacks." Risk Analysis, Vol. 7, No. 1, pp. 35-47. doi:10.1111/j.1539-6924.1987.tb00967.x.

McEntire, D. A. (2005). "Why Vulnerability Matters: Exploring the Merit of an Inclusive Disaster Reduction Concept." Disaster Prevention and Management, Vol. 14, No. 2, pp. 206-222. doi:10.1108/09653560510595209.

McGill, W. L. (1957). "How a State Prepares for Disaster." The Annals of the American Academy of Political and Social Science, Vol. 309, No. 1, pp. 89-97. doi:10.1177/000271625730900112.

McGill, W. L., Ayyub, B. M., and Kaminskiy, M. P. (2007). "Risk Analysis for Critical Asset Protection." Risk Analysis, In press.

Modarres, M., Kaminskiy, M., and Krivtsov, V. (1999). Reliability Engineering and Risk Analysis: A Practical Guide. Marcel Dekker.

Moore, D. A., Fuller, B., Hazzan, M., and Jones, J. W. (2007). "Development of a Security Vulnerability Assessment Process for the RAMCAP Chemical Sector." Journal of Hazardous Materials, Vol. 142, No. 3, pp. 689-694.

NIICIE (2007). "CARVER2®: Critical Infrastructure Assessment Tool." National Infrastructure Institute Center for Infrastructure Expertise. Available at: http://www.ni2ciel.org/CARVER2.asp.

Neale, D., Jackson, E., and Coghlan, G. (2007). "Vulnerability Assessment." Wiley Handbook of Science and Technology for Homeland Security, In press.

Pate-Cornell, E., and Guikema, S. (2002). "Probabilistic Modeling of Terrorist Threats: A Systems Analysis Approach to Setting Priorities Among Countermeasures." Military Operations Research, Vol. 7, No. 4, pp. 5-23.

Paton, D., and Johnson, D. (2001). "Disasters and Communities: Vulnerability, Resilience, and Preparedness." Disaster Prevention and Management, Vol. 10, No. 4, pp. 270-277. doi:10.1108/EUM0000000005930.

Pinto, J. T., Blockley, D. I., and Woodman, N. J. (2002). "The Risk of Vulnerable Failure." Structural Safety, Vol. 24, No. 2-4, pp. 107-122. doi:10.1016/S0167-4730(02)00020-6.

Pluchinsky, D. (2002). "The Heard it All Here, and That's the Trouble." Washington Post, June 16, p. B03.

Reid, S. G. (1992). "Acceptable Risk." in Blockley, D. I. (ed.). *Engineering Safety*, McGraw-Hill. ISBN:0077075935.

Rinaldi, S., Peerenboom, J., and Kelly, T. (2001). "Complexities in Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies." *IEEE Control System Magazine*, December, pp. 11-25.

Roach, J., Ekblom, P., and Flynn, R. (2005). "The Conjunction of Terrorist Opportunity: A Framework for Diagnosing and Preventing Acts of Terrorism." Security Journal, Vol. 18, No. 3, pp. 7-25. doi:10.5555/sj.2005.18.3.7.

Sagan, S. D. (2004). "The Problem of Redundancy Problem: Why More Nuclear Security Forces May Produce Less Nuclear Security." Risk Analysis, Vol. 24, No. 4, pp. 935-946. doi:10.1111/j.0272-4332.2004.00495.x

Sarewitz, D., Pielke Jr., R., Keykhah, M. (2003). "Vulnerability and Risk: Some Thoughts from a Political and Policy Perspective." Risk Analysis, Vol. 23, No. 4, pp. 805-810. doi:10.1111/1539-6924.00357.

Shackle, G. L. S. (1969). Decision, Order, and Time in Human Affairs. 2nd Ed. Oxford University Press. ISBN:521077117.

Vatsa, K. S. (2004). "Risk, Vulnerability, and Asset-Based Approach to Disaster Risk Management." Vol. 24, No. 10-11, pp. 1-48.

Vellani, K. (2006). Strategic Security Management: A Risk Assessment Guide for Decision Makers. Elsevier. ISBN:0123708974.

Villagrán de León, J. C. (2006). Vulnerability: A Conceptual and Methodological Review. Studies of the University: Research, Council, Education, No. 4, UNU Institute for Environment and Human Security (UNU-EHS).

Weichselgartner, J. (2001). Disaster Mitigation: The Concept of Vulnerability Revisited." Disaster Prevention and Management, Vol. 10, No. 2, pp. 85-94.

Westrum, R. (2004). "Increasing the Number of Guards at Nuclear Power Plants." Risk Analysis, Vol. 24, No. 4, p. 959. doi:10.1111/j.0272-4332.2004.00499.x

Woo, G. (1999). The Mathematics of Natural Catastrophes. Imperial College Press. ISBN:1860941826.

Vulnerability Assessment of Arizona's Critical Infrastructure*

Todd White, Samuel T. Ariaratnam, and Kraig Knutson

Abstract: A common theme currently echoed throughout the world is the evaluation, consideration, design, and application of protective systems in an attempt to mitigate the potential of a terrorist attack against targeted locations. Emerging intelligence data, risk and vulnerability analyses, use of environmental design standards, consideration of collateral damage, and existing protective design measures are among the various factors to consider when determining appropriate threat levels and developing a threat mitigation and terrorism prevention program. This paper describes the prevention system and current analytical-based methodology used by the State of Arizona to conduct vulnerability assessments and the comprehensive terrorism prevention program that has been implemented to provide a solution to the all-hazards protection concept.

1. DEFINITION OF PROBLEM AND PROJECT MISSION

The original project mission was defined to organize a system to identify and evaluate assets within the State of Arizona relating to Critical Infrastructure, Emergency Support, Key Assets and locations that have been considered to have the potential of being targeted by individuals or organizations who wish to damage, disrupt or adversely effect the State's economy, ability to function or to cause harm to persons who may occupy the targeted locations.

The program goals were established as follows:

- To coordinate Federal, State and Local resources into a statewide asset evaluation and protection system that combines resources from participating agencies into a cohesive program.

- The system would be designed to include: Federal, State and Local Law Enforcement representatives, Fire Personnel, State Planners, National Guard representatives, Native Nations, Regional Government representatives and private corporate interests.

Several existing systems and methodologies were examined and evaluated and found to be inadequate to address the total protection concepts proposed for the program. The efforts from the program participants were developed into a unique protection system that combines the efforts of various disciplines to create a balanced approach to protecting assets within a defined geographic area. The system consists of several components that will be discussed individually to illustrate the total evaluation and protection concept. The components supporting the program

to be discussed include: GABRIEL; PACES; The TVA Site Screening Process; and Design Review/ Design Standards Development.

2. THE GABRIEL PROJECT

The entire protection system is contained under one project umbrella that has been described as the Geospatial Antiterrorism Buffering, Response and Intervention system providing Education and Logistical support (GABRIEL). GABRIEL provides a flexible system to organize and combine the efforts from State and Local Law Enforcement representatives, Fire Personnel, State Planners, National Guard representatives and regional government representatives into a unified system to compile data and critical information on sites that are identified as potential targets of terrorism.

The program promotes communication and training for individuals from private interests and governmental agencies in contemporary protective systems through a combined effort accomplished through design review, development of building design codes and continuing education programs. Local Universities provide assistance in professional development and encourage the efforts of technology based products developers capable of contributing to the program goals. This comprehensive all-hazard approach provides a system that addresses the entire range of potential concerns ranging from basic encroachments from the criminal element to incidents involving weapons of mass destruction to devastating natural events. Enhanced response preparation, training and matched protocols developed by program participants for terrorist events improve the capability of the same response elements when performing rescue and remediation functions.

This system is managed through a central, state sponsored location that provides the platform to launch a series of programs that provide support, equipment and funding for terrorism prevention activities. The unified approach provides participants with the ability to combine resources, develop consistent methods and protocol that provides enhanced emergency response capability.

There are five major components to GABRIEL that are supported by the data gathering and evaluation methodology (Figure 1). The information is maintained in a constant state of evolution to provide participants with current intelligence data and accurate assessments of identified resources.

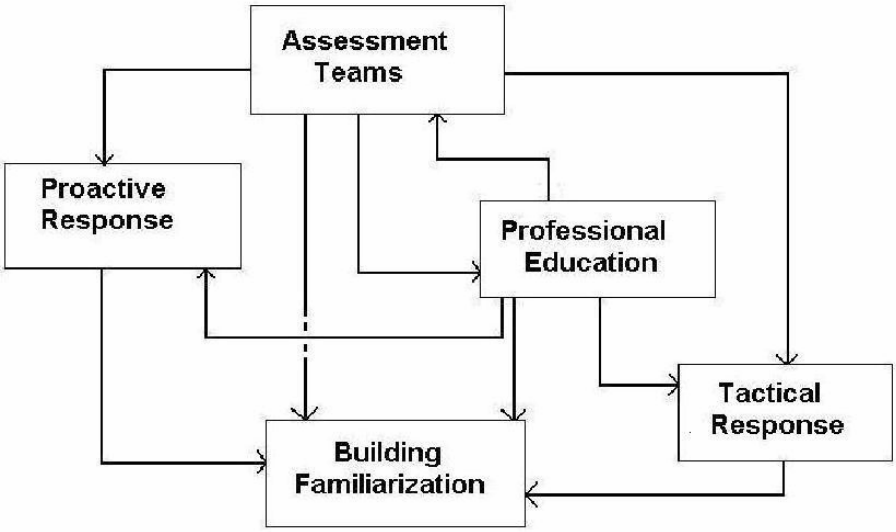


Figure 1. Program Category Interdependence

Figure 1 demonstrates the relationship of the five categories within the program as the information is acquired, developed and disseminated as a working product.

- Assessment Teams: The Assessment Teams perform site assessments, acquire site plans, site data and identify the areas of greatest vulnerability at selected locations utilizing the PACES data system and TVA Site Screening Tools. The teams disseminate information to assist the Proactive Response Teams, Tactical Response Teams and the Building Familiarization Programs. Team members also contribute to the development of appropriate design standards and buildings codes that will further the mission of the program strategy.

- Proactive Response Teams: Proactive Teams receive guidance and direction through information gathered by Assessment Teams and perform counter surveillance operations and proactive patrols at identified sites. Team members also receive training in threat identification, evidence acquisition, preservation and presentation.

- Tactical Response Teams: Tactical Teams are trained and equipped to respond in the most effective and efficient manner to incidents involving acts of terrorism. The participants will be aided in their mission by technology based logistical support systems.

- Professional Education Program: Provides participants with information pertaining to contemporary protective systems and methodology as well assisting Assessment Team Members with the development of applicable design standards and building codes.

- Building Familiarization Program: The information developed by the Assessment Teams is converted into a usable product for team members who conduct exercises and drills with Tactical Response Teams and Fire Personnel at targeted locations for improved coordination in response to incidents.

3. PRIORITIZED ASSET CATEGORIZATION EVALUATION SYSTEM (PACES)

The central data collection methodology and database where information is sorted, stored and digested by the assessment team members in the GABRIEL Program is referred to as PACES (Prioritized Asset Categorization and Evaluation System). This system was developed to provide a fluid method for categorizing and logically prioritizing assets within the designated planning area. In order to arrive at a system that provides an accurate threat picture it was necessary to devise methodology to apply emerging threat intelligence data.

PACES was created to provide that fluid asset categorization and prioritization system for sorting and addressing potential threats, vulnerabilities and for predicting the targeting of sites deemed as possible objects of terrorism or by encroachments from the criminal element. The system provides a method to analyze and apply emerging threats into the evaluation formula in order to provide current and pertinent intelligence data into the system to provide the most accurate image of current conditions and potential threats. The Emerging Threat Indicator (ETI) component of the system, illustrated in Figure 2, allows the data to be evaluated and affected daily as current intelligence information is fed into the database. This provides the most accurate information available that results in a reactive categorization of assets reflecting local and world events that change the nature or source of identified threats.

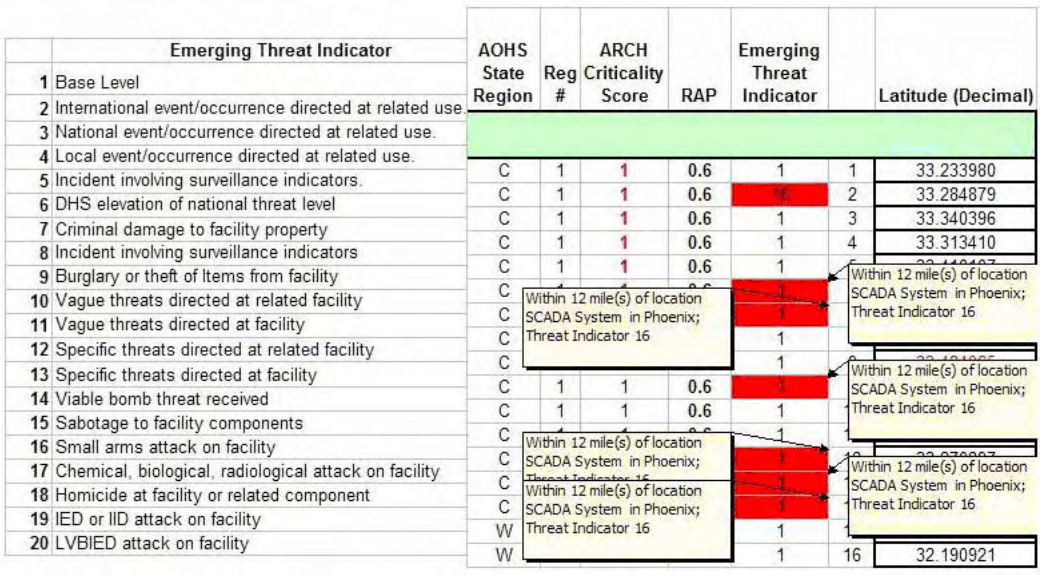


Figure 2. Emerging Threat Indicators

3.1 PACES Classification of Data and Sorting Tools

Basic office software is utilized to form a simple data organization system that is comprised of worksheets combined into a workbook to sort and filter the data into categories. The system has been designed to insure compatibility with the two commonly accepted systems that are currently being used and supported by the U.S. Office of Homeland Security's Office of Domestic Preparedness (ODP). The two accepted systems of categorizing and storing site data: The Homeland Security Critical Asset Management System (HLS CAM); and the Automated Asset Management System (ACAMS) utilize two separate scoring systems to evaluate and identify points of concern at selected sites. HLS CAM uses the CARVER system scoring system while ACAMS uses the MSHARRPP + V system. The PACES System caries this concept further by applying both scoring methodology to insure that the maximum amount of effort has been directed at identifying the considerations that may compel or motivate potential attackers. An enhanced version of the HLS CAM system, CARVER STEPS, provides eleven factors for consideration while MSHARRPP + V utilizes nine criteria for evaluation. The sites are scored individually on both systems after having been divided into Tiers or Sector (defined by the nature of the site function). Population data is also a factor in evaluating the potential area of effect of the sites and is applied to the system by the RAP (Relative Associated Population) formula. Figure 3 illustrates the relative associated population comparison.

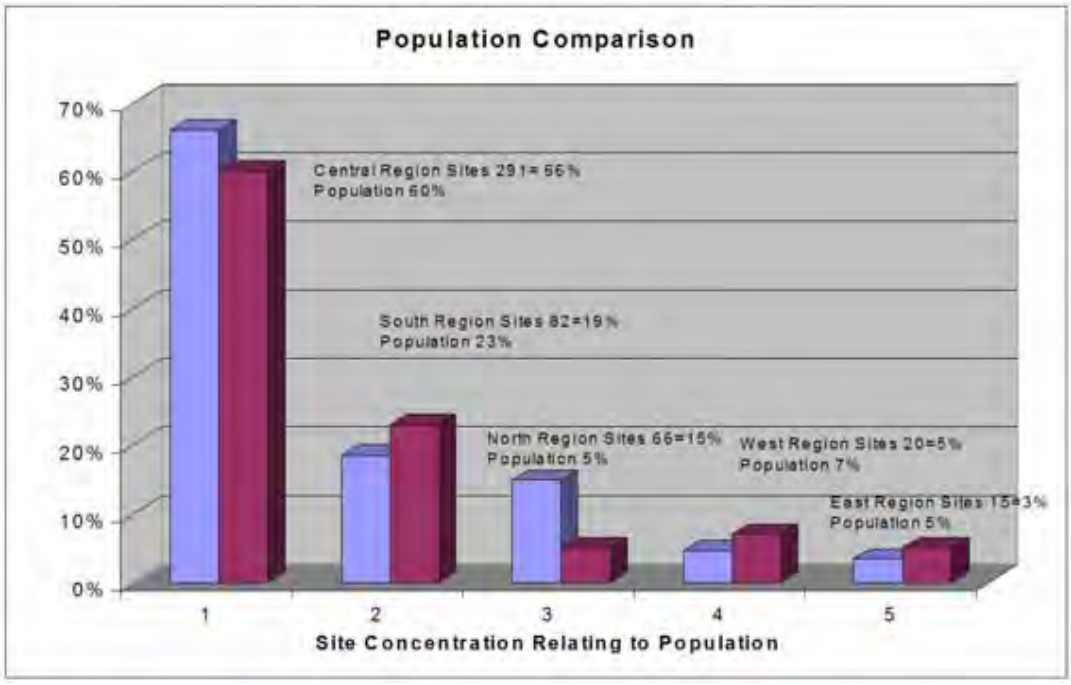


Figure 3. Relative Associated Population Comparison

The system has been designed to support and direct resources managed in order to provide a comprehensive protection plan addressing the all-hazard approach to threat mitigation to insure that adequate response planning is accomplished for the

broadest spectrum of potential events. PACES provides for a flexible system to organize and combine information gathered through the efforts of the Assessment Teams comprised of Law Enforcement representatives, Fire Personnel, State Planners, National Guard representatives and regional government representatives into a unified system. The concepts promoted through the implementation of these programs are designed to allow for the integration of software and the inclusion of information systems that have been promoted by the U.S. Office of Homeland Security.

4. THREAT AND VULNERABILITY ASSESSMENT (TVA) SCREENING TOOLS

The TVA Screening Tools were created in a simple format to provide site evaluation teams with a methodology to quickly identify the problematic areas. By using this layered screening process, an evaluator may quickly assess the most likely source of threat and the greatest vulnerabilities at the selected location. There are three layers that are utilized for this aspect of the site evaluation process.

The forms are basically a series of screening tools that allow a progressive narrowing of focus for the evaluator or assessment teams. The layers are placed in a four page Excel workbook with a summary sheet that allows for a quick comparison of the three scores derived from the three layers of evaluation. The first layer addresses basic site design issues. The second layer addresses site vulnerabilities to threats from criminal acts. The third layer becomes a bit more complex and focused on site vulnerabilities to threats from terrorist attacks.

The TVA Screening Tools were designed to evaluate existing facilities. However, the evaluation process can be used for new buildings during the design process, as well as retrofitting applications of existing buildings undergoing renovation. The three layers of evaluation can be used to assist planners, architects and engineers to identify the best and most cost-effective terrorism mitigation measures for each facility's unique security needs.

The evaluation factors on each level can be perceived uniquely by each evaluator based upon their independent experience and area of expertise; however, this influence can add a broader response to the process which can be balanced through the averaging of scores on the site comparison chart. The subsequent layers of evaluation become increasingly complex in the data evaluated. Color-coded fields, using conditional formatting, assist in readily identifying the areas of highest concern. The scores on layers two and three also provide a value as a percentage, which may be used to allocate resources to the areas of greatest concern. A complete evaluation process using the three levels provides the data for determining relative levels of vulnerability and risk. Each layer progressively includes additional information that will assist in developing solutions to the areas of vulnerability that are identified.

4.1 Layer One - CPTED Rating

The CPTED Rating is designed utilizing the concepts utilized in *Crime Prevention Through Environmental Design* (CPTED). This system will allow the evaluator to obtain a numeric value for the items that have been reviewed for each site. This will provide a methodology for identifying areas in need of design remedy and aspects of the development that should receive closer scrutiny.

Using the system involves the evaluator in assessing each of the ten areas of concern by assigning a numerical value for each of the items listed for consideration under each of the ten main categories. Enter the numerical rank (1 through 5); 1 indicating the most effective approach and 5 indicating the least effective. The score and color will be calculated and applied automatically. The numerical value of 1 to 5 in each of the areas of concern is based upon the evaluator's estimation and assignment of a value in each of the listed subjects.

The ten areas to be evaluated on the form include: Site Function; Open Space; Perimeter/Zone Protection; Visibility/Surveillance Opportunities: Lighting: Established Zones; Communication; Emergency Responders and Hazardous Materials. The corresponding values for each of the items are automatically transferred to the scoring chart. The column is totaled and the sum is reflected in the total score presented in Figure 4.

Element	Score
1	12
2	6
3	3
4	36
5	24
6	30
7	6
8	3
9	36
10	36
CS	192
Total Score	**192**

Figure 4. Layer One Summary Column

4.2 Layer Two - Site Evaluation-Criminal Threat Potential

The purpose of the second layer of screening is to provide a numerical value to define abstract concepts that will assist in identifying areas of concern. The second layer of the process expands the areas of evaluation addressed on layer one and begins to address a wider scope of concerns and provides criteria to identify the targeted area of potential criminal threats to the site.

Layer two calculates and identifies the areas of greatest concern and provides a corresponding numerical value for the selected site that may be used for comparison, design review or for prioritization of the assignment of resources. The summary table is shown in Figure 5.

Estimate the value of each of the identified areas of concern for each of the elements. Enter the numerical rank (1-5, 1 indicating the most effective and 5 indicating the least effective). The associated risk number and color will be calculated and applied automatically as presented in Figure 6.

The evaluator scores each of the sub-categories in the six areas of concern for the following five threat types:

1. Threat to Constructed Element
2. Inventory Threat
3. Data Threat
4. Revenue Threat
5. Personnel Threat

The six areas of concern to be evaluated and the sub-categories for each area are as follows:

1. Site Function
2. Open Space
3. Perimeter/Zone Protection
4. Lighting
5. Established Zones
6. Landscaping

Evaluation of Components	Threat to Constructed Elements	Inventory Threat	Data Threat	Revenue Threat	Personnel Threat
1. Site Function	18	24	6	36	48
Location	3	2	2	4	4
Adjacent Uses	2	3	3	3	3
Supporting Development	1	1	3	2	2
Community Ties	3	4	1	3	4
2. Open Space	10	2	9	16	75
Perimeter/Outer Zone	5	1	1	1	5
Inner Zones/Core	1	1	3	4	5
Building Envelope	2	2	3	4	3
3. Perimeter/Zone Protection	6	96	72	96	160
Perimeter/Outer Zones	3	3	4	3	5
Inner Zones/Core	1	4	3	4	4
Alarm Systems	1	4	3	4	4
Manned Security	2	2	2	2	2
4. Lighting	36	36	12	60	60
Perimeter/Outer Zones	3	3	1	3	3
Inner Zones/Core	3	3	3	4	4
Building Envelope	4	4	4	5	5
5. Established Zones	5	6	24	60	60
Perimeter/Outer Core	5	3	4	3	5
Inner Zone/Core	1	1	2	4	3
Building Envelope	1	2	3	5	4
6. Landscaping	6	18	24	12	8
Perimeter/Outer Zone	3	3	4	2	2
Inner Zone/Core	2	2	2	2	2
Building Envelope	1	3	3	3	2

Figure 5. Layer Two Summary Table

	B	C	D	E	F	Row Sum	Weight	Average	Add'l Factors	
1	18	24	6	36	48	132	12.04%	26.4	1	1
2	10	2	9	16	75	112	10.22%	22.4	2	2
3	6	96	72	96	160	430	39.23%	86	4	3
4	36	36	12	60	60	204	18.61%	40.8	3	4
5	5	6	24	60	60	150	13.69%	30	3	5
6	6	18	24	12	8	68	6.20%	13.6		
CS	81	182	147	280	411	1096	100.00%	2.6		
								13	<Value of greater Than 15 will indicate an area of concern.	
					Overall	Score		221.8		

Figure 6. Corresponding Values Automatically Transferred to the Scoring Chart

4.3 TVA Assessment Layer Three - Terrorist Risk and Vulnerability

The purpose of the third layer of the process is to provide additional information that will be utilized in the identification of points of vulnerability and the calculation of risk in greater detail. The third layer of the process expands the areas of evaluation addressed on layer two and begins to address potential threats from terrorism concerns and provides criteria to identify the targeted area of possible threats to the site.

The worksheet calculates and identifies the areas of greatest concern and provides a corresponding numerical value for the selected site that may be used for comparison, risk and vulnerability identification and for prioritization of the assignment of resources.

The scoring and evaluation of the value of each of the identified areas of concern for each of the elements has changed on this layer. The numerical rank has changed to (1-5, 1 indicating "very low" and 5 indicating "very high"). The risk number and color will be calculated and applied automatically through conditional formatting on the assigned cells. Figure 7 illustrates a Layer 3 summary table.

The numerical value of 1 to 5 in each of the areas of concern is based upon the evaluator's estimation and assignment of a value indicating the: "Asset Value", "Threat Rating" and "Vulnerability Rating" of in each of the listed subjects. The evaluator rates each of these three sub-categories in the six areas of concern: Asset Value, Threat Rating and Vulnerability Rating.

The six areas of concern on level three are as follows:

1. Nature of Site Usage - The assigned mission for the facility. Does the nature of the assigned mission cause the site to be particularly attractive as a potential target of terrorism?

2. Level of Visibility - Is the facility readily identifiable by the nature of its location, building design, signage, significance in the community or through advertising and media accounts? Is it apparent and therefore attractive as a potential target due to its level of visibility?

3. Political/Religious Significance - Does the site represent or serve a political or religious function or interest?

4. Public Venue - Is the site a source of public interest or place of gathering? Are there large populations that frequent the location? Is the site readily accessible and intended for public use?

5. Infrastructure Support Rating - Does the site have value in the infrastructure of the community? Is the location involved in providing infrastructure services such as governmental operations, utilities supply (water, electric, gas), health services or transportation services?

6. Hazardous Materials Present - Are hazardous materials utilized or stored on the site? Is the location involved in the distribution or transportation of hazardous materials? Could the site be targeted due to the nature of the material utilized or stored at the facility?

The five categories of threat to be rated are as follows:

1. Inventory Threat - Threats to materials, products, stored goods or goods in transit that are on the site and could potentially be targeted for theft, damage or a method to disrupt the business. Could materials on the site be targeted as a component for a plan to target another site?

2. Cyber Attack/Data Threat - Internal or external threats to computer systems, stored data, electronic records or businesses or facilities that rely heavily on their computer systems. Does the site house a system be targeted as an attempt to affect other aspects of the business operation? Does the site store critical information or valuable data on the site?

3. Armed Attack/ Pedestrian Bomber - Threats posed by an armed assailant, arsonist or bomber. Includes an individual or group targeting the facility utilizing hand-held weapons. An individual or group who delivers, causes to be delivered, places or carries an explosive device or incendiary device on, near or into the facility.

4. Vehicle Bomb - A vehicle borne explosive device. Is the selected location accessible and vulnerable to a vehicle that could deliver an explosive charge?

5. CBR (Chemical-Biological-Radiological) Attack - Threats posed by an assailant or subject who delivers, causes to be delivered, places or carries a chemical, biological or radiological material or dispersal device on, near or into the facility.

Critical Infrastructure/Potential Target (Risk Rating)	Inventory Threat	Cyber Attack/ Data Threat	Armed Attack/ Ped Bomber	Vehicle Bomb	CBR Attack
1. Nature of Site Usage	4	6	24	36	24
Asset Value	2	3	2	3	2
Threat Rating	1	2	3	4	4
Vulnerability Rating	2	1	4	3	3
2. Level of Visibility	6	18	48	60	60
Asset Value	2	3	4	3	5
Threat Rating	3	3	3	4	4
Vulnerability Rating	1	2	4	5	3
3. Political/Religious Significance	6	6	36	60	48
Asset Value	3	1	4	3	4
Threat Rating	2	3	3	4	4
Vulnerability Rating	1	2	3	5	3
4. Public Venue	6	24	36	60	40
Asset Value	3	3	4	3	2
Threat Rating	1	2	3	4	4
Vulnerability Rating	2	4	3	5	5
5. Infrastructure Support Rating	3	24	16	24	18
Asset Value	3	4	4	2	2
Threat Rating	1	3	2	3	3
Vulnerability Rating	1	2	2	4	3
6. Hazardous Materials Present	24	24	18	48	18
Asset Value	2	2	2	3	3
Threat Rating	3	3	3	4	2
Vulnerability Rating	4	4	3	4	3

Figure 7. Layer 3 Summary Table

4.4 Summary Worksheet

The scores accumulated on the three layers are depicted on the summary sheet of the workbook to allow a method for easy comparison and review of the data. Review of the information allows the evaluator to immediately identify the greatest area of concern based upon the scores from the individual layers (Figure 8). In this example, the highest score is demonstrated on layer one, indicating that the greatest source of problems at this site are the result of basic CPTED design issues.

Summary of Evaluation Layers	
Layer	Score
Layer One	339
Layer Two	201
Layer Three	184.13
Sum	724.13
Average	181.03

Figure 8. Summary Worksheet Score Comparison

5. DESIGN REVIEW AND DESIGN STANDARDS DEVELOPMENT

There have been numerous attempts to promote the establishment of accepted standards for Site Protection Systems that can be applied by Architects, Engineers and Designers as they consider the most appropriate and practical methods for implementation of threat mitigation measures at specific locations. Currently there are no universally accepted building codes or accepted design standards relating to security design or terrorism prevention measures that apply across the board to all types of developments or retrofitting applications. There are, however, protective design standards that are applicable to newly constructed Governmental structures or leased properties under mandates that have been established by the General Services Administration (GSA) and the Department of Defense (DoD). There are also a number of agencies and organizations in existence that have formed and promoted their own protections programs and standards such as those utilized by the Federal Emergency Management Agency (FEMA), the National Fire Protection Association (NFPA), the United States Air Force, the United States Army, the Department of State (DOS), the American Society for Industrial Security (ASIS) and the Center for Disease Control (CDC). However, the mandated application of protective design components or systems to civilian developments does not currently exist outside of jurisdictions that require the inclusion of Crime Prevention through Environmental Design methodology.

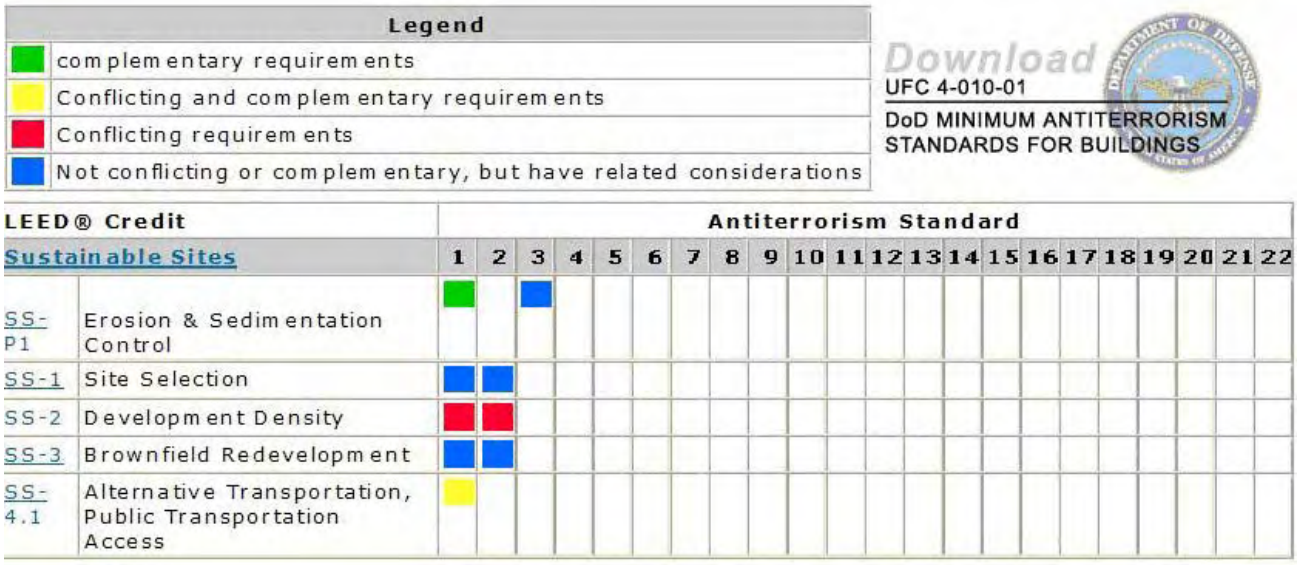
5.1 Whole Building Design Concepts

Whole building design concepts that promote cooperation and communication among the various entities involved in the creation of a new facility are beneficial and encouraged. Whole-building design is a design philosophy that promotes planning to incorporate the coordination of all building components during the design phase of a project. It is intended to integrate all of the subsystems and components of the building to work together as efficiently as possible.

5.2 LEED-DoD Antiterrorism Design Standards Tool

Design professionals have recognized the need for the development of a nationwide system that will encourage the voluntary participation of developers and designers by providing incentives for inclusion of protective design components through an organized system similar to the LEED System that has been developed and promoted by the Green Building Council and the Department of Energy. LEED provides a complete framework for assessing building performance and meeting sustainability goals.

A further development in the expansion of the LEED system that merges Whole Building Design Concepts with ISC Design Standards and DoD Antiterrorism Standards has been accomplished by the implementation of the LEED-DoD Antiterrorism Standards Tool shown in Figure 9.



Legend
complementary requirements
Conflicting and complementary requirements
Conflicting requirements
Not conflicting or complementary, but have related considerations

LEED® Credit		Antiterrorism Standard																						
Sustainable Sites		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
SS-P1	Erosion & Sedimentation Control																						
SS-1	Site Selection																						
SS-2	Development Density																						
SS-3	Brownfield Redevelopment																						
SS-4.1	Alternative Transportation, Public Transportation Access																						

Figure 9. LEED DoD Anti-Terrorism Tools

6. CONCLUSIONS

The effective protection of resources from the threat of damage from human made and natural hazards is a daunting task. A balanced approach involving the consideration of: Protection Measures; Response Capability; Education and Effective Planning will require a unified commitment from all participants. The attitude of Governmental Agencies as well as the design community must remain malleable to react to contemporary events in order to insure that that the optimum balance of design considerations is achieved. To arrive at this goal, coordination with the members of the community is critical. Many asset protection objectives can be achieved during the early stages of the design process when mitigation is the least costly and most easily implemented. Planners, architects, engineers and landscape designers play an important role in working with law enforcement and fire protection specialists in identifying and implementing crucial asset protection measures while considering land use; site selection; the orientation of the buildings on the site; and the integration of vehicle access, control points, physical barriers, landscaping, parking, and protection of utilities. The application of Design Standards is a useful tool in narrowing the options of consideration for design solutions. Advancements in the LEED program are very promising and this system provides a useful cross-reference to DoD Design Standards. However, these “standards” are simply reference points to provide assistance in developing design solutions. They are not intended to be and should not be considered as absolute solutions. Each design problem is unique and must be approached with an open mind. It is important to remember that the nature of threats is fluid and ever changing. The threat will vary depending on the nature of the site and a myriad of related factors. Although indications of potential threats may be scarce during the design stage, consideration should be given to accommodating enhanced protection measures in response to future threats that may emerge. It will be necessary to maintain a vigilant course in pursuing the information received through intelligence sources to constantly reflect

accurate responses to the existing level of potential threats and to design creative and appropriate solutions to mitigate that threat.

Todd White is currently in his 19th year of public service with the Phoenix Police Department and serves as a Detective assigned to the Threat Mitigation Unit at the Arizona Counter Terrorism Information Center (ACTIC). He also served on the Department's Bomb Squad, Patrol Bureau, South Resource Bureau Detective Unit, and Operational Support Unit. Previously, he worked for the Architectural/ Engineering firm of Howard, Needles, Tammen & Bergendoff in Phoenix, Arizona.

At ACTIC, Mr. White has developed and managed a series of critical infrastructure protection programs which provide resources for first response personnel across the State of Arizona by improving response capability, logistical support, and the implementation of threat mitigation measures through improvements in building design. He has also developed a series of data systems designed to coordinate and manage efforts directed at protecting critical infrastructure.

Mr. White is a certified Hazardous Materials Technician and Bomb Technician, and is a member of the American Institute of Architects, American Society of Civil Engineers, International Society of Explosive Engineers, and the International Association of Bomb Technicians and Investigators. He holds a Bachelor of Science in Design in Architecture and Urban Development from Arizona State University and continues to participate in programs at the University.

Samuel T. Ariaratnam, Ph.D., P.E. has served as an Associate Professor at Arizona State University's Del E. Webb School of Construction, Ira A. Fulton School of Engineering, since 2001. In this position, he also performs research in the areas of sustainable urban underground infrastructure systems, infrastructure management and rehabilitation, and trenchless construction methods. Previously, Dr. Ariaratnam served as a faculty member in the Department of Civil and Environmental Engineering (CEE) at the University of Alberta, and as Visiting Assistant Professor and Lecturer in the CEE Departments of the United States Air Force Academy and University of Illinois at Urbana-Champaign, respectively.

Dr. Ariaratnam has over 150 published articles and technical papers, and co-authored books on horizontal directional drilling and pipe bursting. He acts as a journal reviewer for various industry journals, and is a member of numerous professional associations, including the American and Canadian Societies of Civil Engineers and International and North American Societies for Trenchless Technology.

Dr. Ariaratnam holds both a Ph.D. and Master of Science in Civil Engineering from the University of Illinois at Urbana-Champaign and a Bachelor of Applied Science in Civil Engineering from the University of Waterloo.

(see next page)

Kraig Knutson, Ph.D., I.E., CPC has been a member of the faculty of Arizona State University's Del E. Webb School of Construction since 1998, serving as an Assistant Professor and Senior Lecturer. Dr. Knutson previously worked as an Industrial Engineering Research Assistant at Motorola, and an Industrial Engineer and Electrical Engineer at Intel.

Dr. Knutson has authored and co-authored many published works, including textbook language on Construction and Culture and papers presented at both national and international conferences. He acts as a referee for numerous archival journals, including the International Journal of Production Research and Journal of Construction Education, among others. Dr. Knutson is also a member professional construction and engineering associations such as the American Institute of Constructors, American and Canadian Societies of Civil Engineers, American Association of Cost Engineers, American Society of Safety Engineers, and Institute of Industrial Engineers.

Dr. Knutson holds a Ph.D. in Industrial Engineering, Master of Science in Construction, and Bachelor of Science in Construction from Arizona State University.

REFERENCES AND STANDARDS

Department of Defense (2003). *(DoD) UFC 4-010-01 United Facilities Criteria Minimum Standards for Buildings*, United States Department of Defense, October 8, Washington, DC.

Department of Defense (2002). *(DoD) UFC 4-022-01 United Facilities Criteria Security Engineering Entry Control, Facilities Access Control Points*, United States Department of Defense, May 25, Washington, DC.

Federal Emergency Management Agency (2003). *FEMA RM426 Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*, December, Washington, DC.

Federal Emergency Management Agency (2002). *FEMA RM386-7 Integrating Human Caused Hazards into Mitigation Planning*, September, Washington, DC.

Krauthammer, Theodore (2003). "Long Term Research and Development and Educational Needs in Protective Science and Technology Key Note Paper." *Proceedings of the First International Conference on Design and Analysis*, Tokyo, Japan.

Mays, G.C. and Smith, P.D. (1995). *Blast Effects on Building Design to Optimize Resistance to Blast Loading London*, Thomas Telford Publishing, London, UK.

United States Air Force (2004). *HB10-2401 Force Protection Battlelab Vehicle Bomb Mitigation Guide*, January, Washington, DC.

United States Air Force (2003). *Installation Force Protection Guide*, Washington, DC.

United States Army (2001). *Field Manual FM 3-19.30 Physical Security*, January 8, Washington, DC.

United States Army (1998). *AR 525.13 Antiterrorism Force Protection (AT/FP) Security of Personnel, Infrastructure and Critical Resources*, September 10, Washington, DC.

* This paper was previously presented at the 1st Specialty Conference on Disaster Mitigation hosted by the Canadian Society for Civil Engineering (CSCE/SCGC) in Calgary, Alberta, Canada from May 23-26, 2006. The information presented herein has not been updated since the paper's original publication.

Managing Risk in Critical Infrastructures Using Network Modeling

Thomas J. Mackin, Rudy Darken, and Ted G. Lewis

Abstract: This paper outlines the use of network analysis to prioritize and protect critical infrastructures. In this method, graphical networks are used to represent infrastructure systems where key components of the infrastructure are represented as nodes while the interconnections between components, both within and across sectors, are represented as links. Following a risk-based approach, nodes and links are assigned values associated with their vulnerability to specific attack modalities, the dollar cost of consequences associated with removing that node or link, and an investment function related to the costs to harden the node or link. A technique called *critical node analysis* is used to identify the most important nodes and links and to calculate the minimum risk possible given limited resources. This technique has been applied to a variety of infrastructures across critical infrastructure and key resource (CI/KR) sectors as diverse as water, energy (power), telecommunications, information technology (Internet), and transportation systems to determine what is critical in each of these sectors.

The critical node analysis technique provides the analyst with three key results: (1) identification of critical nodes and links, (2) optimal allocation of limited resources to minimize risks, and (3) identification of network failure modes. We demonstrate the general utility of the method by detailing its application to the Kinder Morgan transmission pipeline in Southern California.

CRITICAL INFRASTRUCTURE AND RISK MANAGEMENT

In 1996, President Clinton established the President's Commission on Critical Infrastructure Protection (PCCIP), chaired by Robert Marsh. The resulting "Marsh Report," released in October 1997 and formally titled "Critical Foundations: Protecting America's Infrastructures," was the first to define "infrastructure" as "a network of independent, mostly privately-owned, man-made systems and processes that function collaboratively and synergistically to produce and distribute a continuous flow of essential goods and services." The Marsh Report also identified "critical infrastructures" as infrastructures "so vital that their incapacity or destruction would have a debilitating impact on our defense and economic security" (President's Commission on Critical Infrastructure Protection 1997, 3).

The work of the PCCIP prompted President Clinton to issue Presidential Decision Directive 63 (PDD-63) in 1998 (Office of the President of the United States 1998), which defined, more specifically, our Nation's critical infrastructure and identified eight basic sectors. Following the terrorist attacks of 9/11, President Bush, in July of 2002, released the "National Strategy for Homeland Security" (Office of the President of the United States 2002). Shortly thereafter the administration released "The

National Strategy for the Physical Protection of Critical Infrastructures and Key Assets" (Office of the President of the United States 2003) which expanded the list of critical infrastructure sectors and key resources to 14. The 2006 publication of the National Infrastructure Protection Plan (NIPP) identified 17 specific critical infrastructure and key resource (CI/KR) sectors as well as assigned agency responsibilities (see Table 1) (Department of Homeland Security).

TABLE 1. Critical Infrastructure and Key Resource Sectors as of 2006

Sector	Lead U.S. Department
Agriculture and Food (Meat and poultry - Department of Agriculture) (All other food products - Department of Health & Human Services)	Department of Agriculture Department of Health & Human Services
Defense Industrial Base	Department of Defense
Energy	Department of Energy
Public Health and Healthcare	Department of Health & Human Services
National Monuments and Icons	Department of the Interior
Banking and Finance	Department of the Treasury
Drinking Water and Water Treatment Systems	Environmental Protection Agency
Chemical Commercial Facilities Dams Emergency Services Commercial Nuclear Reactors, Materials, and Waste	Department of Homeland Security *Office of Infrastructure Protection*
Information Technology Telecommunications	Department of Homeland Security *Office of Cyber Security and Communications*
Postal & Shipping	Transportation Security Administration
Transportation Systems	Transportation Security Administration, U.S. Coast Guard
Government Facilities	Immigration and Customs Enforcement, Federal Protective Services

The application of network analysis to describe critical infrastructure was motivated by the definition of a critical infrastructure, in government publications, as a ***network*** of components that operate "***collaboratively*** and ***synergistically*** to produce and distribute a ***continuous flow*** of ***essential*** goods and services" (emphasis added). These italicized words will be key as we describe why critical node analysis is so effective at identifying critical components of an infrastructure.

The implementation of the national strategies requires a detailed understanding of the Nation's infrastructure. Whoever implements a critical infrastructure protection strategy, however, runs headlong into a formidable problem: our infrastructure is vast. Indeed, each sector defined in Table 1 is extremely large and complex. The telecommunications sector alone contains billions of components. The gas and oil systems within the energy sector contain more than 250,000 miles of pipeline. The various supply chains making up the food, transportation, and chemical industries are so vast and complex that it is difficult even to estimate their size! This complexity is compounded further when we account for the interdependencies between sectors. Taken together, as the collection of sectors is so expansive, it would require trillions of dollars to protect every component of every sector.

The National Research Council (NRC) made explicit this fact in its 2002 publication , "Making the Nation Safer: The Role of Science and Technology in Countering Terrorism," where it stated, "Our society is too complex and interconnected to defend against all possible threats." Instead, the NRC called for a risk-based approach to countering terrorism. This approach was embraced by Department of Homeland Security (DHS) Secretary Chertoff, who, in testimony before the Senate Committee on Homeland Security and Governmental Affairs on September 12, 2006, stated:

> *First, it's important to make sure we are focused on the most significant risks to our homeland and that we apply our resources in the most practical way possible to prevent, protect against, and respond to both man-made and natural events.*
>
> *No matter how hard we may try, we cannot eliminate every possible threat to every individual in every place at every moment. And if we could, it would be at an untenable cost to our liberty and our prosperity. Only by carefully assessing threats, vulnerabilities, and consequences, and prioritizing our resources, can we fully ensure the most practical and optimized protection for Americans and our nation.*

It is clear that the only practical strategy to best protect the Nation is to identify the most critical components of our infrastructure and protect those first. The key question, then, is how we do so. A risk-based approach to homeland security requires a national consensus on the approach used to measure risk, where all stakeholders, both public and private, agree on the methodology. Secretary Chertoff, in his March 9, 2005 testimony before the Senate Committee on Homeland Security and Governmental Affairs, stated:

> *I want to emphasize that our philosophy, our decision-making, our operational activities and our spending will be grounded in risk management as we determine how best to prevent, respond and recover from attacks.*

In general, risk is defined as:

$$R = T*V*C \qquad (1)$$

Where: T (threat) is the likelihood that a specific attack scenario will be attempted against a given asset,
V (vulnerability) is the probability of success of the specific threat against the asset, and
C is the consequence of asset failure.

Both threat and vulnerability are measured as probabilities in the range of [0, 1], while consequence can be measured as the dollar cost of consequences, loss of life, loss of public confidence, etc. In any case, special skills are required to determine any of the three inputs to the risk calculation. Vulnerability to an attack mode requires special knowledge of the facility and its means of failure, weaknesses, protections, etc. This requires engineering knowledge of how the asset functions and what might happen if the asset is attacked in a specific manner. This will certainly require a knowledgeable assessment team with access to detailed facility information and may well require sophisticated red-teaming. Threat is the most difficult input parameter to measure since it requires human Intel to determine adversary capabilities, intent, and goals, all of which are laced with inherent uncertainties. Nonetheless, threat is an essential part of the risk calculation and is an important consideration in the DHS risk-based investment strategy.

The risk associated with our entire infrastructure would be the sum of risk over all assets and over all threat scenarios. It is clear that such a problem becomes exceedingly large. Furthermore, though the risk-based approach is the only rational path to securing our infrastructure, the absence of a common framework for modeling infrastructure, calculating vulnerabilities, and estimating consequences has impeded greatly our national goal of protecting critical infrastructure. After more than five years of refinement in the definition of critical infrastructure, there remains little understanding of specifically which assets are critical in a critical infrastructure sector. The method presented here addresses this by providing the policy-maker with a general approach as well as a set of tools for identifying the truly critical components in any sector that can be represented as a network. Additionally, we provide a rigorous method of minimizing sector risk by allocating resources to the most vital portions of the sector. Finally, we show how critical node analysis can be used to prevent or minimize cascade failures in CI/KR sectors such as water, energy (power), telecommunications, information technology (Internet), and transportation systems.

1. CRITICAL NODE ANALYSIS

Critical node analysis provides answers to two key questions: (1) what is critical in an infrastructure? and (2) what is the best allocation of limited resources to sector components such that the sector's risk is minimized? It begins by modeling a sector as a collection of nodes and links (Lewis 2006). In physical infrastructure, nodes are typically associated with infrastructure components while links are relationships among pairs of nodes. In other contexts, nodes and links represent more abstract entities. For instance, a human network would model people as nodes and their social relationships as links. For the purposes of this article, we use concrete examples where physical assets make up the network.

The purpose of modeling a critical infrastructure as a network is to determine which nodes and links are critical to the continuity of the network. We define critical nodes as the "most vital" assets in the network, and critical links as the "most vital" links. Quantifying how "vital" a node or link is provides a measure of the impact on the entire network if that node or link is destroyed or disabled.

Latora and Marchiori (2004) were the first to apply the idea of node criticality to a network model of an infrastructure. They analyzed the Infonet Internet backbone communications network and the 9/11 hijacker's social network using network *efficiency* as a metric of criticality. In their analysis, network efficiency was defined as the inverse of the shortest distance between any two nodes. As a network is damaged, either by loss of nodes or links, it is obvious that the path to connect any two nodes will either increase or remain the same, with a similar change in network efficiency.

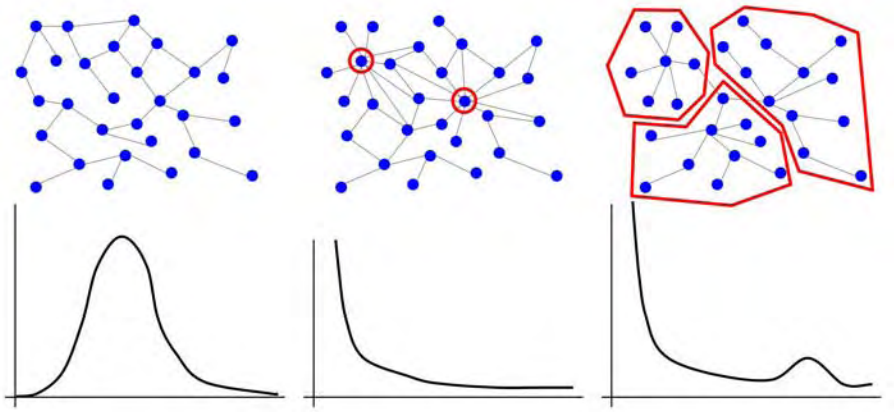
Latora et al. define *critical nodes* as those that contribute the most to the change in the overall network efficiency. That is, nodes are ranked – from highest to lowest – according to their effect on network efficiency, where the highest-ranking nodes are the most critical. Though attractive for its simplicity, this approach has two key shortcomings: (1) it does not include the structure of a network, and hence does not allow for the impact of node removal on the overall network topology, and (2) it ignores the relative value of a link or node – that is, it assumes all nodes are of equal value, and ignores completely the value of links.

Apostolakis and Lemon (2005) use a similar technique to model infrastructure as a network of nodes and links, but identify the minimal cut sets that contain critical nodes. In this model, the minimal cut set is defined as "a set of events (usually failures) that guarantee the interruption of service." Unfortunately there can be a rather large number of cut sets to consider in a modest sized network. For example, Apostolakis and Lemon analyzed a natural gas distribution network containing 23 nodes and found over 1,000 cut sets!

Our definition of a critical infrastructure network is similar to the definition used by Apostolakis and Lemon, but the analysis techniques are quite different. We both assign a value to each node, but, instead of using cut sets to identify critical nodes,

we use network risk to determine critical nodes and links. The primary difference in the techniques is that the topology of the network determines the cut sets in Apostolakis' and Lemon's approach while our approach identifies the highest-valued nodes and/or links. Furthermore, our approach identifies the optimum investment strategy to reduce the overall network risk.

Research has shown that network topology is important when deciding the criticality of nodes and links (Barabasi 2003; Dezso and Barabasi 2002; Pastor-Satorras and Vespignani 2001). In general, networks are broadly classified as one of three particular types: (1) scale-free, (2) random, or (3) small world (see Figure 1).



(a) Random (b) Scale-free (c) Small World

FIGURE 1. Schematic representations demonstrating the general shape of the three primary types of networks (upper) and histograms showing how the number of links varies with each type of network: (a) random network with no visible structure, (b) scale-free network with the hubs circled, and (c) small world network with three neighborhoods outlined.

As noted above, a scale-free network is one whose distribution of links to nodes obeys a power law, which means the most highly connected nodes are the most rare, but also the most important. Scale-free network theory has been used to explain a number of physical and social phenomena, but its relevance here stems from the fact that the most-heavily connected nodes are more important to the integrity of a network. Clearly, removal of highly-connected nodes does more to dismantle the network than removal of less-connected nodes.

In a scale-free network, critical nodes are the ones with the highest connectivity, i.e., they are the nodes with highest degree. In fact, the most critical node is the node with maximum degree. However, scale-free network analysis is not sufficient in the context of infrastructure protection because it does not address the relative value of nodes and links. In physical infrastructures, some nodes are worth more than others, requiring the definition of criticality to include the relative value of nodes and links. In the approach presented here, which we call critical node analysis, and an associated model using a software suite we have named "model based risk assessment (MBRA)," we combine the structural information of scale-free network

analysis with the target value of nodes and links associated with infrastructure components.

In order to demonstrate critical node analysis, we present an analysis of the Kinder Morgan petroleum transmission system that supplies Southern California with gasoline and other petroleum products (see Figure 2) (see Lewis 2006). This network contains nine nodes (terminals and junctions), and the necessary transmission pipes that connect terminals and junctions. Clearly, this infrastructure can be modeled as a network where nodes are terminals and junctions, and links are pipes, resulting in nine nodes and eight links.

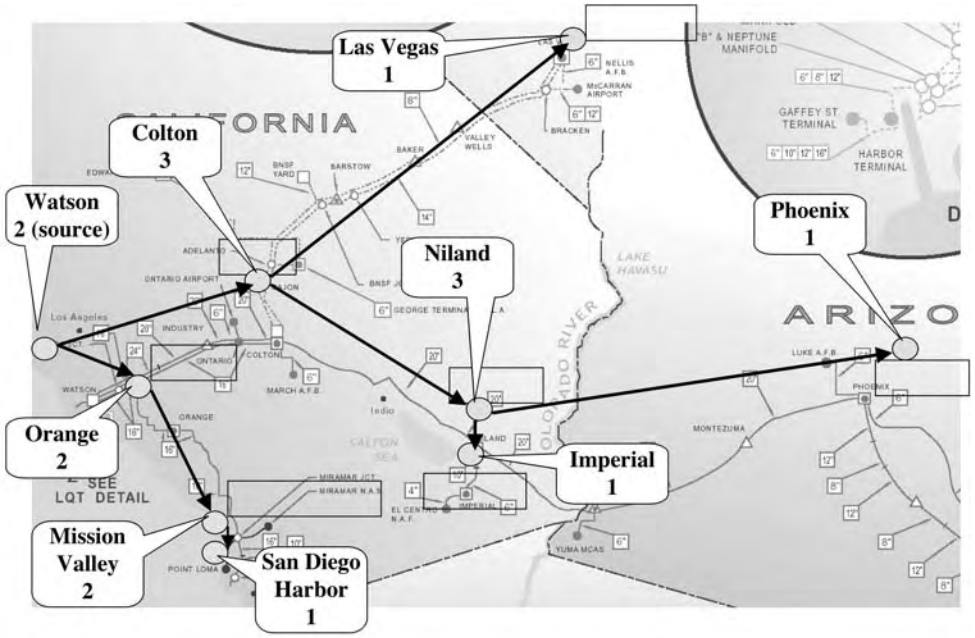


FIGURE 2. The Kinder Morgan transmission network supplies petroleum products to Southern California, Nevada, and Arizona.

Though this is a relatively simple infrastructure, it would be prohibitively expensive to protect every mile of pipeline and every yard of perimeter around terminals and junctions. Instead, we ask, what is most critical in this infrastructure? We identify what is critical by calculating the risk associated with each component. The policy-maker can then decide to protect only critical nodes, while limiting or eliminating the expense of protecting all nodes and links.

Critical node analysis is derived from probabilistic risk analysis (PRA) initially developed for use in the aerospace and nuclear reactor safety fields (Bedford and Cooke 2001). PRA requires that the analyst identify the events that may lead to failure of a component, and estimate the probability and consequences of failure of each component. This is summarized using a fault tree, a logical construction that exhaustively models the ways that a given asset can fail and includes the probabilities and consequences associated with each type of failure. For example, the Watson facility in Figure 2 might fail due to an earthquake, or attack by a terrorist

using a bomb, or a power failure, etc. We label these events QUAKE, BOMB, and POWER FAILURE and place them into a fault tree diagram (see Figure 3). In this case, the various failure causes are connected by a logical "OR" gate – that is, the occurrence of any one of these events could bring the Watson terminal down. Note, however, that the power system includes a back-up, so bringing the power down requires that the facility loses both the line power and the back-up power. This part of the fault tree illustrates the effect of redundancy or resiliency. An asset is more resilient if its fault tree is assembled from "AND" gates – that is, it is harder to bring down an asset that requires multiple points of attack. Figure 3 is not intended to be exhaustive, but to illustrate that a fault tree is a logical construction that allows the user to connect all possible causes of failure. One might imagine that it can be exceedingly complex. To be quantitative, it must include the likelihood of each event's occurrence and also include the associated damages resulting from each given event. Using this, along with the probabilities of each event's successful impact, we can estimate the probability of failure of any asset, including the Watson terminal.

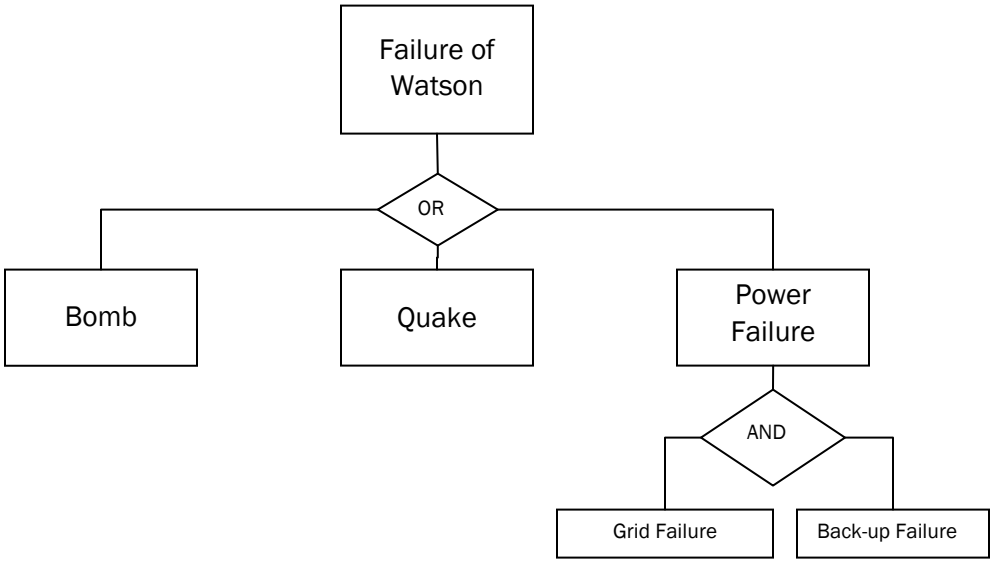


FIGURE 3. Example fault tree for the Watson terminal showing threats connected by logical gates.

Though fault trees are an essential part of understanding how assets fail, they do not tell us how critical the Watson terminal is to the entire network of Figure 2. In Figure 2, we might assign a probability of failure for Watson that addresses both BOMB and QUAKE events and use fault tree analysis to analyze the Watson node in more detail, as we did in Figure 3. But, what about the other nodes and links in Figure 2? Even if we use a much simpler estimate of probability of failure, we must still include the effect of link and node failures on the overall security of the pipeline system. The solution to this problem is to consider the connections – as well as individual nodes and links – when computing risk.

PRA can model multiple components and multiple events – not merely single components and events –so it could be expanded to the entire network in Figure 2, which contains nine nodes and eight links as components. Typically, a fault tree is expanded into a corresponding event tree that enumerates all possible combinations of single and multiple events. A fault tree with *k* events generates an event tree with 2^k events. Therefore, the fault tree for Figure 2 expands into an event tree with $2^{(9+8)}$ = 128,000 events!

If we apply PRA to an infrastructure system represented by nodes and links in a network, we would have to construct a very large fault tree containing all nodes and links of the network and then use the PRA method to obtain the overall network risk. Clearly, this approach is not practical. Instead, we must first determine the criticality of our nodes and links in the network so as to reduce the problem to the subset of nodes and links that are most vital to network function. That is, we use a network approach to reduce the complexity of the problem, and construct fault trees only for those nodes and links that are critical to overall network performance. The following paragraphs outline how this is done.

Let the *vulnerability* be the probability, p(i), of failure of a component (node or link), *i*, when the component is attacked. Vulnerability may be different for different kinds of attacks. For example, p_{bomb}(pipeline) = 20% means that a certain portion of the Kinder Morgan pipeline will fail with probability 0.2 when attacked by a bomber. Similarly, p_{power}(Watson) = 25% means the Watson terminal will fail with probability 0.25 when power is cut off. Vulnerability depends on the kind of threat juxtaposed against a sector's component as well as the likelihood that the attack will succeed. Again, this is not the probability that an asset or component will be attacked, it is the probability that an attack will succeed. That is, our network analysis assumes that an asset has been targeted for attack. Therefore p(i) is the probability of a successful attack, assuming the attack takes place. Consequently, probability values in critical node analysis may seem high at first glance. For example, p(power substation) = 50% may imply that the substation has some protection but can be successfully targeted about half the time, while p(transformer) = 100% implies that transformers in the open are completely unprotected and can always be disabled if targeted.

Risk was defined in Equation 1 to include threat. Threat is the probability that a specific asset, or group of assets, will be attacked using a specific attack mode. To simplify our analysis, we assume a conditional risk assessment, where the threat probability is 1, and the risk is simplified as vulnerability times damage: r(i) = p(i)d(i), where d(i) is the expected damage to asset *i* caused by a successful attack. For example, if the average repair cost of a bombed pipeline is $10,000, and p_{bomb}(pipeline) = 0.2, then the risk associated with a successful attack on a pipeline is given by: r(pipeline) = 0.2 (10,000) = $2,000. As mentioned above, we can also calculate the downstream economic impacts of damage and include these numbers in the cost of consequences. For the purpose of illustration, however, we have simplified our damage estimates.

Equation 1 does not account for the "connectivity value" of a node or link within a network. For example, removal of Niland in Figure 2 impacts three links and their attached nodes (Colton, Phoenix, Imperial), while removal of Imperial impacts one node and one link. Clearly, more connected nodes have a bigger impact on the overall system than less connected nodes – this is the idea behind critical node analysis. Network risk must include the connectivity of nodes as well as their vulnerability, *v*, and consequence value, *d*. This requires a modification to the fundamental risk equation:

$$R = \sum_j g_j \cdot v_j \cdot d_j \qquad (2)$$

Where: *v* is vulnerability,
d is damage, and
$g_j = 1$ if it is a link, otherwise g_j is the degree of the node (how many links are connected to it).

What is special about network risk is that the number of links associated with any given node (node degree) raises the number of times that a node must be counted in a fault tree. As a result, the degree of the node plays an important role in the value of that node to the network and appears as a multiplier in the risk equation.

Network risk, *R*, defaults to simple risk when $g_j = 1$, which makes this definition attractive while accommodating the intrinsic connectivity of a network. Obviously, scale-free networks contain hub nodes with a high g_j value, which means hubs are more critical to the overall network (see Figure 1(b)). Similarly, non-hub nodes are less critical, because $g_j = 1$. Conversely, if the damage value of a non-hub node is high, then the impact to the overall network is $g_j * d_j$, – a significant amount for large d_j. Therefore, network risk models both of the aforementioned factors contributing to risk – the connectivity as well as the damage.

For a given system, g_i and d_i are set, and v_i is to be determined. Note that we are constrained to a fixed budget, *b*, which limits how much "protection" we can allocate to each node and link in the network. If the budget is large, we can reduce the vulnerability so that risk is minimal. If the budget is small, we can reduce vulnerability somewhat, but not close to zero. The objective of critical node analysis is to minimize the risk, *R*, by optimal allocation of a limited budget to "buy down" vulnerability. The larger the budget, the smaller the risk.

2. RISK MINIMIZATION

The key question is: How do we allocate our budget, *b*, to minimize the overall risk to the network? Assuming an initial vulnerability of $v_i = 100\%$ for all nodes and links, what is the best way to distribute the budget to protect nodes and links by reducing the vulnerability? Al-Mannai and Lewis (2007) recently provided a closed-form solution to the optimization problem above for two cases: (1) when vulnerability v_i is a linear function of funding, and (2) when it is an exponential function of funding. We

have written a comprehensive software suite that includes network analysis, fault tree analysis, and resource allocation, the Model Based Risk Assessment (MBRA). The software is available for download in the public-domain and can be accessed by contacting the authors.

2.1. Application to Kinder Morgan

Returning to Figure 2, applying the optimizing principle to the Kinder Morgan network results in identification of its critical components and also tells us the best utilization of resources to protect the critical assets of the network. As an illustration, suppose the damage value of all nodes and links is set to 50, except for Watson, which is set to 100, because it is the source for the entire network flow. The logic here is that roughly one-half (50 of 100) of the petroleum flowing from Watson goes to Orange, and the other half to Colton.

Now, suppose the budget is b = 100. Obviously, all 100 points should go to protect Watson, because it supplies product flows to all other nodes and links. But, if the budget is b = 200 points, linear allocation reduces vulnerability of Watson, Colton, and Niland! Orange, as well as all links, receives 0 points. In other words, Watson, Colton, and Niland are the critical nodes in this critical infrastructure, in rank order according to the product of $g_i * d_i$.

Again, what is critical in a critical infrastructure? – the high-degree and high-value nodes and links. Identification of these critical nodes and links reduces the problem of protecting critical infrastructure to protecting critical nodes – a much more manageable problem.

3. CONCLUSIONS

Critical node analysis extends earlier results of scale-free network analysis by incorporating damage values at each node and link into the network representation of a critical infrastructure sector. This has the added benefit of identifying what is critical in a critical infrastructure, and, furthermore, addresses the important question of "What is the best allocation of resources that minimizes risk?" The key feature of the analysis is that the risk equation is modified to include the degree of the node. This modification accounts for the topology of the network and weights the contribution of every node in the network. In practice, one would use critical node analysis to determine the key assets in a network infrastructure. Once identified, one would go on to construct fault trees for that reduced set of assets. This approach greatly simplifies the analysis and reduces enormously the task of protecting critical infrastructure.

Critical node analysis often yields surprising results when applied to a variety of critical infrastructure sectors. For example, application of this technique to the top tier-1 Internet service providers shows how to protect the 250 million Internet servers throughout the world by hardening fewer than 200 of the critical nodes (Lewis 2006). In general, critical node analysis suggests a radically advantageous strategy: instead

of protecting everything, it is only necessary to protect an extremely small percentage of a vast infrastructure. Critical node analysis reduces the cost and complexity of critical infrastructure protection by exploiting the inherent structure of most sectors. Once this structure is known, it is possible to apply resources, in the right amount, to enhance the security of the most critical nodes and links.

Tom Mackin, Ph.D. is Professor and Chair of the Department of Mechanical Engineering at the California Polytechnic State University, Adjunct Professor in the Naval Postgraduate School's Center for Homeland Defense and Security, and Adjunct Professor of Mechanical Engineering Sciences at the University of Illinois. Previously, he was an Assistant, then Associate, Professor of Mechanical Engineering at the University of Illinois at Urbana-Champaign (UIUC), and worked as a research engineer in the Materials Department at UC Santa Barbara. From 2002-2003, he served as an American Society of Mechanical Engineers (ASME) Executive Office Fellow in the White House Office of Science and Technology Policy, working as a technology policy analyst and White House Liaison to the National Nanotechnology Initiative. In 2004, he became the Founding Director of the Illinois Homeland Security Research Center, and an affiliate faculty member in UIUC's Arms Control, Disarmament, and International Security program.

Dr. Mackin's research interests include structural health monitoring, non-destructive evaluation, advanced composites, micro-electrical-mechanical systems, sensors and detectors, nano-mechanics, scientific instrumentation, science and public policy, and the application of network theory to the protection of critical infrastructure. He has authored over 100 papers and holds 3 patents. He received his Ph.D. in Engineering Science and Mechanics from Penn State in 1991, and is a member of the ASME, American Association for the Advancement of Science (AAAS), and the Materials Research Society (MRS).

Rudy Darken, D.Sc. is the Director of the Institute for Modeling, Virtual Environments, and Simulation (MOVES) and Professor of Computer Science at the Naval Postgraduate School in Monterey, California. He also serves as Director of Research for the Center for Homeland Defense and Security (CHDS). He is an Associate Editor of PRESENCE Journal, the MIT Press journal of teleoperators and virtual environments. He received his B.S. in Computer Science Engineering from the University of Illinois at Chicago in 1990 and his M.S. and D.Sc. degrees in Computer Science from The George Washington University in 1993 and 1995, respectively.

(see next page)

Ted Lewis, Ph.D. currently serves as a Professor of Computer Science and Visiting Professor of National Security Affairs at the Naval Postgraduate School in Monterey, CA. Additionally, he is the Executive Director and Academic Associate for the School's Center for Homeland Defense and Security. Dr. Lewis has a 30-year publication record consisting of over 100 refereed and non-refereed publications, and has held board memberships and editorships for numerous magazines published by the Institute of Electrical and Electronics Engineers, Inc. (IEEE). Dr. Lewis received both his M.S. and Ph.D. in Computer Science from Washington State University, and his B.S. in Mathematics from Oregon State University.

REFERENCES

Al-Mannai, W. I. and Lewis, T. G. (2007). "Minimizing Network Risk with Application to Critical Infrastructure Protection." Journal of Information Warfare, Vol. 6, Issue 2, August, pp. 52-68.

Apostolakis, G. E. and Lemon, D. M. (2005). "A Screening Methodology for the Identification and Ranking of Infrastructure Vulnerabilities Due to Terrorism." Risk Analysis, Vol. 25, Issue 2, April, pp. 361-376.

Barabasi, A. (2003). Linked: How Everything Is Connected To Everything Else and What It Means for Business, Science, and Everyday Life. Plume Books.

Bedford, T. and Cooke, R., (2001). Probabilistic Risk Analysis: Foundations and Methods. New York: Cambridge University Press, p. 390.

Department of Homeland Security (2006). National Infrastructure Protection Plan.

Department of Homeland Security (2005). Testimony by Secretary of Homeland Security Michael Chertoff Before the Senate Homeland Security and Governmental Affairs Committee. March 9.

Department of Homeland Security (2006). Testimony of Secretary Michael Chertoff U.S. Department of Homeland Security Before the Senate Committee on Homeland Security and Governmental Affairs. September 12.

Dezso, Z. and Barabasi, A. (2002). "Halting Viruses in Scale-free Networks." Physical Review E, Vol. 65, 055103-(R).

Holland J.H. (1996). Hidden Order: How Adaptation Builds Complexity. New York: Addison-Wesley.

Latora, V. and Marchiori, M. (2004). "How the Science of Complex Networks Can Help Developing Strategies Against Terrorism." Chaos, Solitons & Fractals, Vol. 20, Issue 1, April, pp. 69-75.

Lewin, R. (1992). Complexity: Life at the Edge of Chaos. New York: MacMillan.

Lewis, T. G. (2006). Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation. John Wiley & Sons, pp. 388-390, 504.

National Research Council of the National Academies (2002). Making the Nation Safer: The Role of Science and Technology in Countering Terrorism. Washington, D.C.: The National Academies Press, p. 2.

Office of the President of the United States (1998). Presidential Decision Directive 63.

Office of the President of the United States (2002). National Strategy for Homeland Security.

Office of the President of the United States (2003). The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.

Pastor-Satorras, R. and Vespignani, A. (2001). "Epidemic Spreading in Scale-free Networks." Physical Review Letters, Vol. 86, pp. 3200-3203.

President's Commission on Critical Infrastructure Protection (1997). Critical Foundations: Protecting America's Infrastructures.

Stiber, N. A., Small, M. J., and Pantazidou, M. (2004). "Site-Specific Updating and Aggregation of Bayesian Belief Network Models for Multiple Experts." Risk Analysis, Vol. 24, Issue 6, December, pp. 1529-1538.

U.S.-Canada Power System Outage Task Force. (2004). Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations.

Waldrop, M. M. (1992). Complexity: The Emerging Science at the Edge of Chaos. New York: Simon and Schuster.

Wikipedia (n.d.). Emergence. Retrieved July 15, 2005 from http://en.wikipedia.org/wiki/Emergence

Same Words, Different Meanings: The Need for Uniformity of Language and Lexicon in Security Analysis and Risk Management

Andrew G. Harter

Abstract: As the security analysis and risk management field grows and professionalizes, practitioners face a sincere problem. Methodology and terminology have grown and incubated in a number of government agencies, companies, and academic circles without sufficient overlap, resulting in confusion, misunderstanding, and incompatibility of findings. This article takes a strategic look at the problem, including issues with current approaches, how standard-setting methodology applies to this scenario, and a case study approach to resolving the issue.

"Police officers responded to a domestic dispute, accompanied by marines. They had just gone up to the door when two shotgun birdshot rounds were fired through the door, hitting the officers. One yelled 'cover me!' to the marines, who then laid down a heavy base of fire. . . . The police officer had not meant 'shoot' when he yelled 'cover me' to the marines. [He] meant . . . point your weapons and be prepared to respond if necessary. However, the marines responded instantly in the precise way they had been trained, where 'cover me' means provide me with cover using firepower. . . . over two hundred bullets [were] fired into that house."[1]

During the Los Angeles riots in 1992, troops from the California National Guard and United States Marines from 1st Marine Division at Camp Pendleton were deployed to assist the Los Angeles Police Department. This meeting of security practitioners from different sectors gives a clear and dramatic example of the problems caused by the lack of common lexicon, meanings, and terminology.

Without a doubt, the most commonly voiced obstacle to progress in the field of security analysis and risk management is the lack of a common vocabulary, used consistently, even by a simple majority of practitioners. This causes confusion in its mildest forms and, in more severe instances, prevents comparison of analyses due to conflicting assumptions. Lack of comparability prevents stakeholders from making key decisions, rendering the process of risk management difficult at best.

A common lexicon means developing a set of agreed upon terms and definitions amongst the practitioners in the industry. Common meanings are often developed within cohesive groups where discussion and consensus can be reached naturally through the course of regularly working together. It is when these groups interact with other groups that misunderstandings occur, and a simple misunderstanding of terminology often casts doubt upon an entire methodology, complicating the ability to come together and work collaboratively. This can cause unnecessary conflict and

frustration as practitioners defend their analytical framework instead of the analysis itself, resulting in wasted time and resources, as well as potentially incompatible final products.

While some companies and government agencies have and continue to develop common terminology internally, a profession-wide standard is needed. Any effort within a single government agency or company is by necessity incomplete, as these efforts to develop standardized approaches are not generally accepted beyond the parochial limits of their own subset without the agreement and consensus forged by a wider contributing body. Resolving these problems requires the development of consensus across the entire security analysis and risk management profession. Such a process entails the collection of current definitions from all concerned practitioners and organizations, followed by amalgamation through a consensus-building process that considers majority and minority views in order to attain buy-in from all components that will be expected to utilize the definitions after their formalization.

This problem is not approached in a vacuum – the problem of standards and definitions has to be addressed in all professions and industries as part of their maturation process. Achieving this goal requires an effort to collect input from professionals in all agencies, utilizing a voluntary consensus methodology to add reputability to the resulting standards. Development of a common lexicon is a required foundational element for further evolution of the security analysis and risk management profession. Once a lexicon is established, practitioners can communicate in commonly understood terms and move on to higher levels of maturation, such as the creation of generally-accepted principles, certifiable training, and interoperable analytical results.

In this article, the problems associated with the lack of a common lexicon are discussed before delving more deeply into seeking the solution. This includes why current methodologies for standard-setting have not worked and what the requirements and complications are for moving forward. More specifically, the article will address developing a common lexicon using recognized standard creation methods, and how a consensus process can be applied to be effective. A case study is also provided that highlights the Security Analysis and Risk Management Association (SARMA)'s approach to this issue.

WHY DO WE NEED A COMMON LEXICON NOW?

As was discussed above, lack of common terminology can cause unnecessary divisions and confusion between government agencies and other groups who have developed along parallel paths within the risk management community. Further, companies that deal with multiple agencies or groups often have problems with risk communication and reputability when moving between groups that have different understandings of the same terms.

Companies within the industry can and do take advantage of this problem, undermining the foundation of a competing company's methodology based on core assumptions and semantic differences in order to then market their own solution as a preferred alternative. In reality, all methodologies include certain assumptions in their make-up, and trading one set of assumptions for another without a common baseline to which the methodologies can be compared does not often result in a superior solution – merely the appearance of progress by the acceptance of change.

In addition, as long as methodologies are developed without a baseline of best practices and common meanings, analysts who are skilled and experienced with one set of methods and theories will find themselves without portable skills when they move to another agency or company that uses security risk theory.

Without a common basis for communication and interoperable methodologies, there also are no standards to which training can be molded. The number of people required to be trained and knowledgeable in security analysis and risk management is growing rapidly in the post-9/11 environment and ad-hoc mentorships with experts in the field are not a viable mechanism for training them all. Development of standards amongst the experts of the community also creates a baseline from which education plans can be built, allowing analysts and risk specialists to be trained and students to enter the field with the framework of knowledge necessary to begin establishing a career in this profession.

Most importantly, without a common lexicon and interoperable methodologies, cooperation is inhibited between federal, state, and local agencies, as well as the private sector, and is made less feasible and practicable, even though the problem is resolvable. While an agency may see success due to the interoperability of its own internal units, that success becomes frustration for those outside the agency's boundaries. For example, if a member of private industry aligns itself to the standards of the Department of Defense (DoD)'s Defense Critical Infrastructure Program (DCIP), how is it expected to respond when approached by one of the Department of Homeland Security (DHS)'s critical infrastructure protection components, or react to the requests of the Federal Bureau of Investigation (FBI)'s local Joint Terrorism Task Force (JTTF)? When a state and local fusion center receives mandated standards from the FBI, as well as from DHS and the National Guard, each wanting information on local assets in incompatible formats with different standards for inclusion, who does it respond to? The time, labor, and funding spent on overcoming problems of incompatibility are both substantial and unnecessary, and it is crucial that we overcome them as an industry on our path to a more mature profession.

DEVELOPING STANDARDS: CONSENSUS AND MANDATE

Standardization occurs by one of two mechanisms: *consensus* or *mandate*.

Mandated standards require a singular body with authority over the community to define methods and terms, and with the power and influence necessary over its

constituents to enforce compliance. While this has occurred within individual government agencies where purse strings can influence policy, it is ultimately only effective to the extent of that agency's range of influence. For example, despite the mandated acceptance of the National Infrastructure Protection Plan (NIPP) by DHS, it has little influence on physical security practitioners of DoD or the Department of State. The private sector needs to balance these government requirements with their own needs, further promoting confusion.

At the other end of the spectrum, consensus can occur naturally – common language often grows organically and naturally between groups of practitioners working together. Many entities will standardize within themselves to promote internal efficiency and then encourage others to adopt their standards as well. This process generally works when one organization invents or otherwise possesses a clear lead on activities and can frame the definitions in a way that newcomers then accept. When multiple groups of practitioners develop simultaneously, however, this process grinds to a halt, as each group is reluctant to accept the dictates of an outside group when they conflict with their own internal findings. This is where the security analysis and risk management community finds itself at this time – competing methodologies utilizing competing terminology with no incentive for seeking commonality. Both incentive and a mechanism for standardization are now needed.

Several commonly recognized categories are applicable to mandated and consensus-driven standards:

- *Company standards* are dictated within an individual corporation, and *government standards* are dictated within the government. Both of these are standards governing internal practices of those limited bodies.
- *Industry standards* are agreed upon by all the major actors in a given industry, but without the reasonable input of third parties, consumers, or other concerned entities.
- *Legal standards* are instituted by law and *international standards* instituted by treaty, both of which are widely accepted but rigid and unresponsive.
- *Voluntary consensus standards*, by contrast, are created by open contribution and agreement of all parties, and specifically require that due-process procedures be created to ensure the concerns of all parties are accounted for fairly. This includes widespread participation such that all interested parties can reasonably be considered accounted for, as well as an open forum for unfettered debate and protections for minority viewpoints to ensure full consideration under a consensus, rather than majority, decision-making system.

Voluntary consensus standards have been created in a number of industries, and are deemed to be the most reputable, even if the most time-intensive, standard type to create. The U.S. Government places a high value on the contributions of volunteers and the hard work of consensus-building activities in industry, trade, and standards groups. The National Technology Transfer and Advancement Act of 1995 (NTTAA)[2] mandates that departments of the U.S. Government use the voluntary consensus

standards of non-government agencies, and was clarified[3] to state that this included "the definition of terms" of concern in this article.

For the security analysis and risk management profession, there is currently no body with the authority to mandate and the power to force the acceptance of a single set of definitions upon the industry. This authority may eventually be found and enforced through the White House, such as the National Security Council or Office of the Director of National Intelligence, but at this time the actions necessary for this to occur have not been taken and numerous U.S. Government Accountability Office (GAO) reports and independent findings have not been sufficient to create the political will to enact a process that will function on mandate. Thus, consensus has resulted in numerous corporate or government standards, but a true consensus in the industry has not emerged. Without leadership and direction by a standard-setting body recognized by security analysis and risk management practitioners, it is also unlikely that full consensus standards will emerge.

To address this problem, SARMA is taking the first steps towards gathering input for consensus standards, and as it works to develop a common lexicon for security analysis and risk management professionals, the defined procedures of voluntary consensus standards can be drawn upon to help in the effort.

APPLYING VOLUNTARY CONSENSUS STANDARDS TO RISK MANAGEMENT

In order to be valid voluntary consensus standards, the following criteria need to be met by the organization creating them:

> *A voluntary consensus standards body is defined by the following attributes:*
> *(i) Openness.*
> *(ii) Balance of interest.*
> *(iii) Due process.*
> *(iv) An appeals process.*
> *(v) Consensus, which is defined as general agreement, but not necessarily unanimity, and includes a process for attempting to resolve objections by interested parties, as long as all comments have been fairly considered, each objector is advised of the disposition of his or her objection(s) and the reasons why, and the consensus body members are given an opportunity to change their votes after reviewing the comments.*[4]

These points will be addressed individually in the sections below.[5]

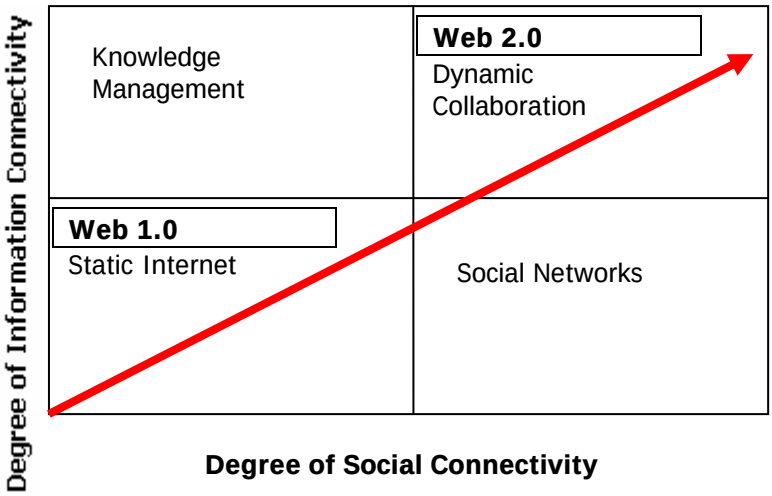
Openness

In order to gather the volunteer base necessary to reach a true voluntary consensus standard, the process needs to be open to all interested parties and permit the democratic flow of ideas. General theory allows that the wider the base of input, the better and more representative the final product will be. Organizations such as the American Society for Testing and Materials (now known as ASTM International), which develops technical standards worldwide, rely on a volunteer membership of

over 30,000 consumers, producers, and experts from the private and public sectors. As previously noted, a wide base of participation is necessary to ensure that all interested parties are accounted for in the consensus process.

A fresh look at this factor shows that new opportunities for openness and new, more enabling technologies are changing the way that business is conducted and the way collaboration can happen. New concepts such as Wikinomics and Web 2.0 are being implemented on the World Wide Web, creating information sharing mechanisms and social networking technologies that can be adapted to meet business needs.

Don Tapscott, author of Wikinomics: How Mass Collaboration Changes Everything, analyzes the new shift in thought occurring in modern business today. The ease of collaboration created by internet evolution is changing the corporate thought model. Rather than the best result coming from the increased collaboration of a single company or government agency getting a few dozen minds together, now it is possible to have hundreds to thousands of contributors working on a problem collaboratively, sharing knowledge to produce a better result. As an example, Proctor & Gamble plans to have 50% of its new product development coming from outside its own research and development office.[6] By moving beyond ownership of ideas to decentralized contribution, better results can be created. To achieve this level of product, business needs to conjoin an asymmetric collaboration network with a method for organizing and capturing knowledge.



The use of MediaWiki open source software has revolutionized the information-gathering capability of many entities. While scalable up to millions of users and records as is done by Wikipedia, the same software has also been put to use within the Department of State to create Diplopedia[7] and by the Director of National Intelligence to produce the interagency Intellipedia.[8] The base functionality of this off-the-shelf tool allows many users to access a single set of documents and edit content in a fully-audited, traceable manner. MediaWiki is an efficient and scalable knowledge management solution offering Wiki-based collaborative opportunities for a wide, open base of interactive input.

The weakness of the Wiki approach is exemplified by Wikipedia, which is widely criticized for the lack of reputability of its contributions. Wikipedia is a free-for-all implementation of this software, resulting in the most persistent (i.e., loudest) voice coming through most often. The implementations of Diplopedia and Intellipedia show how the same software can be used successfully when control and validation tools are added. For use in a common lexicon environment, the Wiki approach allows the widest collection mechanism amongst industry practitioners and professionals, but to meet a standard of reputability and the minority-view consideration required for a voluntary consensus standard, controls of due process are required. These are discussed below.

Due Process

Due process is where the free-wheeling and chaotic atmosphere typically associated with Wikipedia and its associated enterprises ends and the process of building a respected, authoritative, consensus-driven standard begins.

Due process requires that all ideas be fairly heard and considered, all negative votes be fully assessed, and reasonable surety be complied with as a standard is advanced to towards acceptance. As has been cited by other experts, "this tortuous process often takes years to produce a standard."[9] The use of advanced technical means of collaboration cannot be permitted to replace the rigor of this process, but it can greatly facilitate the speed at which collaboration can occur. Handling discussion and casting votes through a robust online forum instead of by mail ballot, for example, can allow for far faster turn-around and examination of results. A proper process of examination places the power in the hands of the entire organization's membership, but ensures the results are coupled with the respect and reputability of its senior elected board. A solid process of evaluation and acceptance ensures the reputability of the standards arrived at.

The evaluation process has the following major steps:

1. Collection of all current definitions (corporate, government, industry, or specialist);
2. Review of definitions to find a consensus;
3. Review of the consensus;
4. Review of all dissenting votes; and
5. Ratification by the organization.

Open access to web-based knowledge management software, such as a Wiki solution, facilitates the first step, with the widest base of interested parties being able to contribute and thus ensure a broad base of input for consensus standards. Online collaboration tools, monitored by project teams, can then go beyond the Wiki limitations by allowing steps two through four to be handled accurately and in a documented fashion so that all minority views are heard, considered, and addressed as required for a voluntary consensus standard. The existence of an organized and recognized body with the authority to oversee steps two through four makes step five

viable, with a documented form of due process making the organization's ratification credible.

Balance of Interest

Balancing interests is what separates a voluntary consensus standard from other forms of standards – industry, corporate, government, etc. It is recognized that industry experts have the greatest interest in achieving the benefits of standardization, and industry standards are therefore often completed. To have a voluntary consensus standard, however, it is necessary that not only producers (in our case, security risk management analysts), but also their consumers (federal, state, and local governments, owners and operators of privately-owned critical infrastructure, etc.) and any interested third parties (academia, general public) have full input in the process.

The purpose of this balancing in a voluntary consensus standard is to address all sides of the issue, and thus approach Pareto optimality[10] with the standard created. Pareto optimality is a measure of efficiency considering all sides of an issue – it is the state at which the outcome cannot be further improved without harming another party. This means, specifically, that it does not arrive at the best solution for industry, but instead the best solution for the producers and the consumers together, based on all sources of input.

One problem with this approach, however, is that a voluntary consensus standard is created by volunteers. Since the economic interests of industry professionals are generally served by the creation of standards, it is understood and accepted that they naturally have a greater interest in participation, and thus often compose the majority of any standard-setting body. To this end, any organization that desires to be a legitimate standard-setting body needs to take steps to reach out to other communities and encourage their participation. The standards body ASTM International, for example, has a set rule that the voting body of a committee cannot be composed more than 50% of producers when it works on developing technical standards.[11] It is imperative that standard-setting organizations establish clear and consistent rules for representation that will imbue their findings with credibility.

The role of due process in protecting a balance of interest comes into play in the crucial role of protecting minority viewpoints. It is necessary to have firm procedures for handling and documenting the consideration of each point of feedback in the consensus process, which allows for a standard to be proposed, then votes to be cast. Each negative vote should be captured, along with the underlying rationale. Then, each negative vote's rationale should be considered by the voting body. Some organizations put each negative vote to an additional vote as to whether its argument is persuasive, and a 2/3 agreement on the persuasiveness of the minority view sends the standard back for additional revision until the committee is satisfied that the concern is addressed. In this way, each minority view is put to the consideration of the whole before a standard moves forward in the process.

Another issue with balance of interest is handling personal interest when arguing matters of public good. It is necessary that people address this "big hat / little hat" issue by setting aside their personal, corporate, or agency roles when discussing standards intended for the good of the whole. While the vast majority of participants are ethical and honorable in their actions, the flexibility built into the consensus system to protect minority viewpoints naturally permits unscrupulous participants to act unethically in attempting to sway a standard in a way that is more favorable to their personal viewpoint. This issue is addressed at length in the Journal of Business Ethics by Mark Marpet,[12] who concludes that the establishment of a clear code of ethical behavior, established and published by the regulatory body is both acceptable, and in fact necessary, to protect the interests of the whole. He goes further to recommend that enforcement standards which allow for action against those found to be acting unethically should be established, with judgment passed by unaffiliated and unbiased membership and removal from participation for repeat offenses. A firm policy established in advance with protections built in to prevent the silencing of minority views but permitting the removal of privileges for repeat offenders will improve the process and also serve to strengthen the reputability of the organization while limiting its susceptibility to legal action.

An Appeals Process

Even when the consensus process reaches a level of stability where it can be sanctioned and published for the use of all members, it is still important that it be open to renewed debate as the circumstances that would affect the Pareto optimal equilibrium arise. It is natural that the publication and distribution of a standard will result in the generation of more concerned parties, which in turn results in the necessary inclusion of more minority viewpoints.

In this vein, consensus standards are essentially "living documents" which can be subject to further contribution, discussion, and dissent as time goes on. Technology helps here once again – by having a flexible media repository capable of receiving threaded and linked discussion, it becomes easy for grassroots discussion to occur amongst the membership and concerned parties, potentially reinitiating a review process within the standards body. Public transparency once again proves to be the strength of a reputable process.

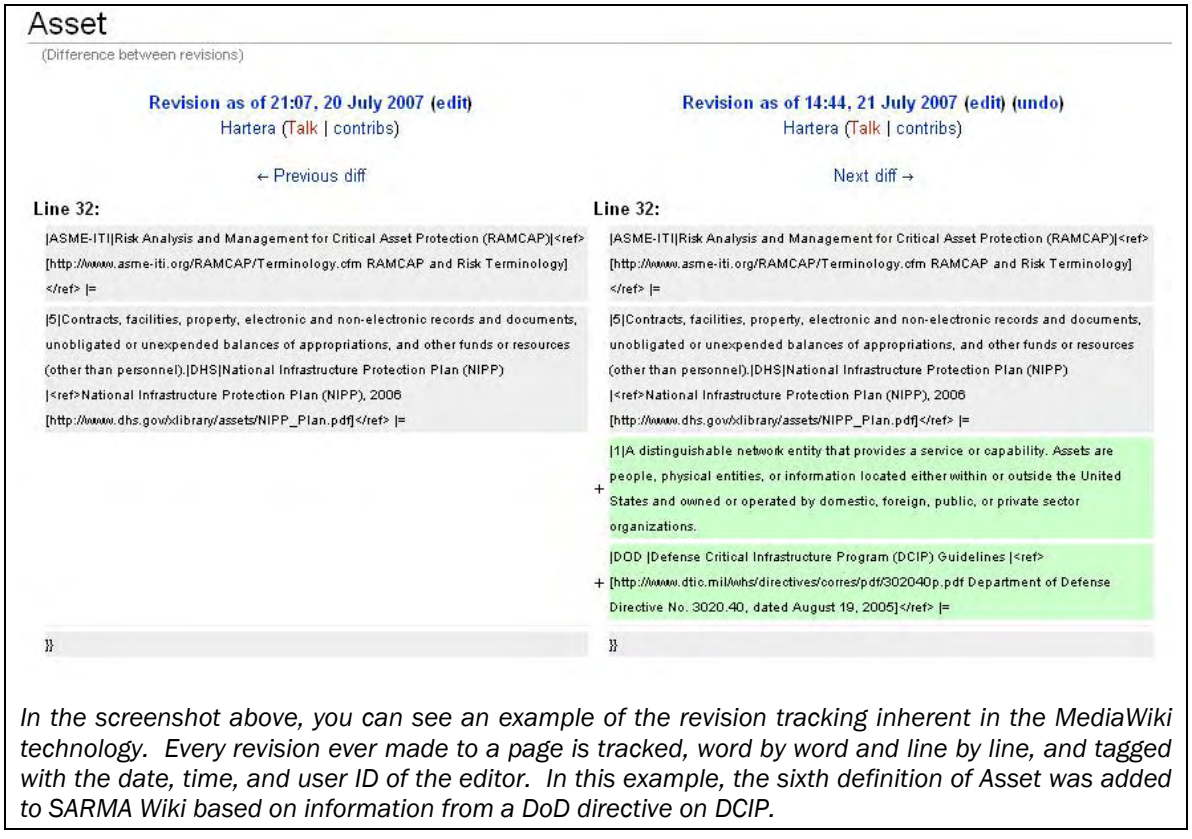
THE SARMA COMMON LEXICON: CASE STUDY

The security analysis and risk management profession has grown exponentially since the events of September 11, with many practitioners developing methodologies, and many government agencies establishing internal standards. Professionals in the field have moved to create SARMA, a non-profit organization dedicated to establishing continuity across the profession. It is SARMA's intent to go beyond the bounds of corporate standards, government standards, or industry standards to create a viable voluntary consensus standard, common to private industry and government alike, that will allow for security analysis and risk management studies and results to be comparable across federal, state, and local agencies, as well as the

private sector. Success in this endeavor will allow for efficiencies across each of these domains by way of public/private cooperation in developing the voluntary consensus standard. SARMA has reviewed the requirements for being considered a standard-setting body under the rules of voluntary consensus standards, and is establishing a mechanism by which consensus standards can be developed for a common lexicon.

Step 1: Technology

SARMA has established a public, accessible web presence at http://www.sarma.org, and a web-based implementation of MediaWiki software at http://www.sarma-wiki.org/ for the purpose of capturing input for its Common Lexicon Project. This knowledge base allows users to come and identify themselves, then edit and add information to a public encyclopedia of security analysis and risk management terms and methodologies. The MediaWiki solution provides the same backbone used by Wikipedia in the public sphere and Intellipedia and Diplopedia inside the U.S. Government, and is scalable up to any size needed without significant constraint. Edits are fully auditable and linked to user accounts, so the source of any edit can be traced by project staff or other users. Threaded comment capability in the software allows for users to continue to add to and comment on the definitions without modifying them once an initial consensus version has been established.


Asset

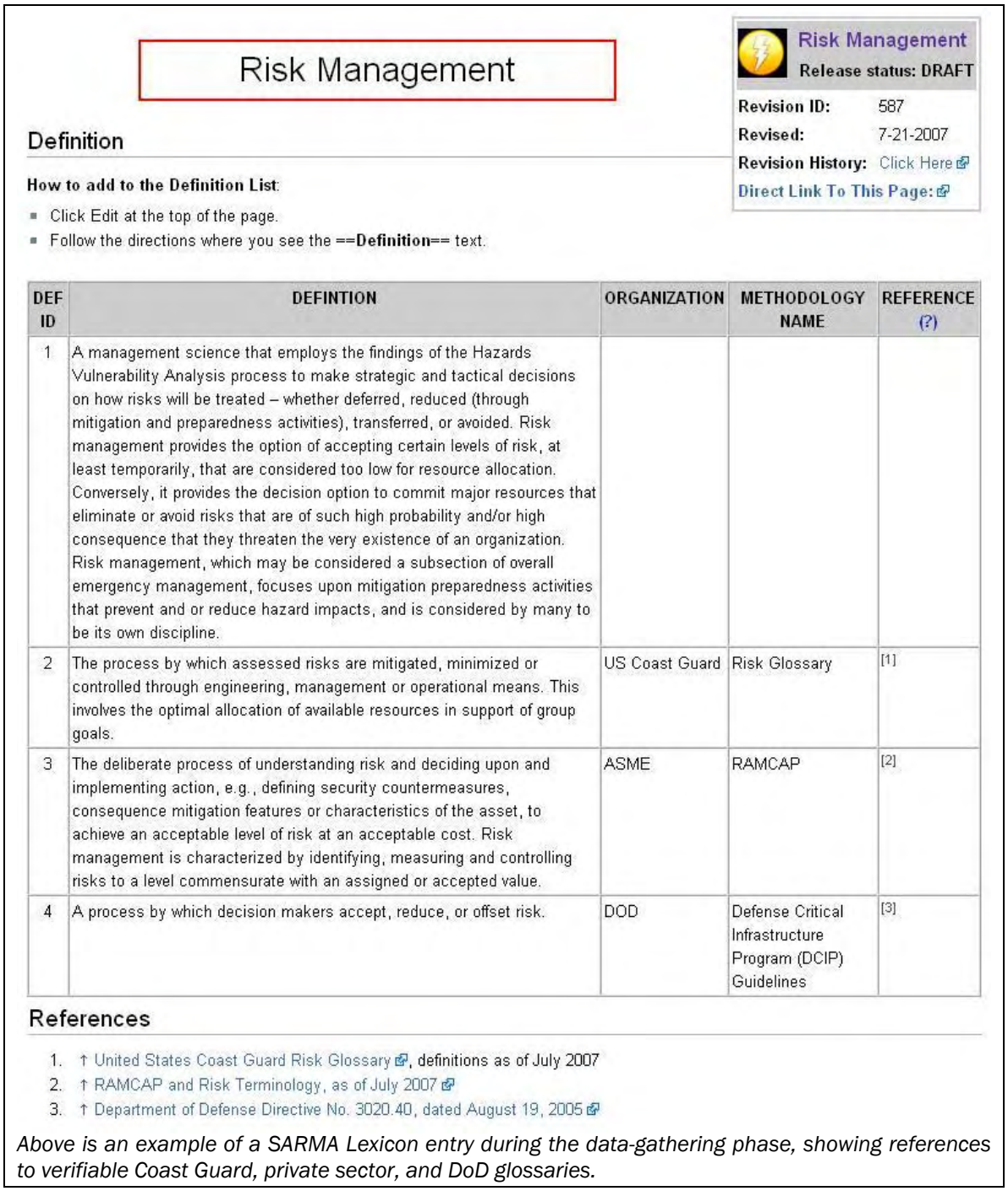
(Difference between revisions)

Revision as of 21:07, 20 July 2007 (edit) Hartera (Talk | contribs) ← Previous diff	Revision as of 14:44, 21 July 2007 (edit) (undo) Hartera (Talk | contribs) Next diff →
Line 32:	**Line 32:**
|ASME-ITI|Risk Analysis and Management for Critical Asset Protection (RAMCAP)|<ref> [http://www.asme-iti.org/RAMCAP/Terminology.cfm RAMCAP and Risk Terminology] </ref> |=	|ASME-ITI|Risk Analysis and Management for Critical Asset Protection (RAMCAP)|<ref> [http://www.asme-iti.org/RAMCAP/Terminology.cfm RAMCAP and Risk Terminology] </ref> |=
|5|Contracts, facilities, property, electronic and non-electronic records and documents, unobligated or unexpended balances of appropriations, and other funds or resources (other than personnel).|DHS|National Infrastructure Protection Plan (NIPP) |<ref>National Infrastructure Protection Plan (NIPP), 2006 [http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf]</ref> |=	|5|Contracts, facilities, property, electronic and non-electronic records and documents, unobligated or unexpended balances of appropriations, and other funds or resources (other than personnel).|DHS|National Infrastructure Protection Plan (NIPP) |<ref>National Infrastructure Protection Plan (NIPP), 2006 [http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf]</ref> |=
	+ |1|A distinguishable network entity that provides a service or capability. Assets are people, physical entities, or information located either within or outside the United States and owned or operated by domestic, foreign, public, or private sector organizations.
	+ |DOD |Defense Critical Infrastructure Program (DCIP) Guidelines |<ref> [http://www.dtic.mil/whs/directives/corres/pdf/302040p.pdf Department of Defense Directive No. 3020.40, dated August 19, 2005]</ref> |=
}}	}}

In the screenshot above, you can see an example of the revision tracking inherent in the MediaWiki technology. Every revision ever made to a page is tracked, word by word and line by line, and tagged with the date, time, and user ID of the editor. In this example, the sixth definition of Asset was added to SARMA Wiki based on information from a DoD directive on DCIP.

Step 2: Gathering Data

As of December 2007, SARMA's staff is in the data-gathering stage of the project, with definitions being collected for about 150 terms thus far. Primary sources containing governmental department standards, corporate standards, and previous consolidations of industry standards continue to be gathered by SARMA volunteers, while an open call to the SARMA membership is issued for the entire membership base to contribute input from individual areas of expertise.



Risk Management

Risk Management
Release status: DRAFT
Revision ID: 587
Revised: 7-21-2007
Revision History: Click Here
Direct Link To This Page:

Definition

How to add to the Definition List:

- Click Edit at the top of the page.
- Follow the directions where you see the ==**Definition**== text.

DEF ID	DEFINTION	ORGANIZATION	METHODOLOGY NAME	REFERENCE (?)
1	A management science that employs the findings of the Hazards Vulnerability Analysis process to make strategic and tactical decisions on how risks will be treated – whether deferred, reduced (through mitigation and preparedness activities), transferred, or avoided. Risk management provides the option of accepting certain levels of risk, at least temporarily, that are considered too low for resource allocation. Conversely, it provides the decision option to commit major resources that eliminate or avoid risks that are of such high probability and/or high consequence that they threaten the very existence of an organization. Risk management, which may be considered a subsection of overall emergency management, focuses upon mitigation preparedness activities that prevent and or reduce hazard impacts, and is considered by many to be its own discipline.			
2	The process by which assessed risks are mitigated, minimized or controlled through engineering, management or operational means. This involves the optimal allocation of available resources in support of group goals.	US Coast Guard	Risk Glossary	[1]
3	The deliberate process of understanding risk and deciding upon and implementing action, e.g., defining security countermeasures, consequence mitigation features or characteristics of the asset, to achieve an acceptable level of risk at an acceptable cost. Risk management is characterized by identifying, measuring and controlling risks to a level commensurate with an assigned or accepted value.	ASME	RAMCAP	[2]
4	A process by which decision makers accept, reduce, or offset risk.	DOD	Defense Critical Infrastructure Program (DCIP) Guidelines	[3]

References

1. ↑ United States Coast Guard Risk Glossary, definitions as of July 2007
2. ↑ RAMCAP and Risk Terminology, as of July 2007
3. ↑ Department of Defense Directive No. 3020.40, dated August 19, 2005

Above is an example of a SARMA Lexicon entry during the data-gathering phase, showing references to verifiable Coast Guard, private sector, and DoD glossaries.

Step 3: Iterative Review

As key definitions receive a critical mass of input and comment, the Common Lexicon Project Team will synthesize the results and work to create a core definition through linguistic deconstruction of the various definitions. A definition, potentially with a series of sector-specific interpretations, will result and be sent to the membership for comment and dissent. An online arena will be ready for threaded discussion on any definition proposal, with all dissenting votes being discussed according to voluntary consensus principles.

This process will involve breaking down the definitions into a single, core definition and weeding out extraneous text to find a common meaning. Since not all sectors in the industry will accommodate a one-size-fits-all approach, some terms may also have sector-specific subsets attached to them as well. Finally, the historical context and usage of various public and private sector terminologies will be archived and referenced so that prior work and manuals can be understood appropriately and compared to current definitions and meanings.

Step 4: Board Review

Once a definition has reached consensus amongst the participating constituencies, it will be submitted to the SARMA Board of Directors for review and approval. While members of the Board may have participated in the discussion process as SARMA members, their duty as part of the Board of Directors is to certify that the discussion and collaboration performed in arriving at the lexicon definition presented to them meets the standards of reputability required for a voluntary consensus standard, and thus can be certified by SARMA.

Step 5: Publication

SARMA will publish the common lexicon periodically in whatever forms are deemed most valuable by SARMA members – printed volume(s), online reference guides, etc. The SARMA Wiki will also be available for future comment, interpretation, or dissent, which will affect future published versions of common lexicon materials. Unlike several other standard-setting bodies, SARMA is a non-profit professional association, and will not copyright or sell the resulting lexicon, instead focusing on sustaining donations and memberships and offering its common findings to the public for free.

CONCLUSIONS

Problems of interoperability and lexicon affect all practitioners in the security analysis and risk management industry, and cause problems for all government agencies and corporations who utilize security risk management techniques in their decision-making. These issues need to be addressed across the industry, overcoming both governmental and corporate boundaries to arrive at common terminology and

baselines to underlie methodology. When successful, both public and private practitioners will benefit from reduced costs of collaboration, interoperability of results, and professionalization of the industry, allowing them to develop new theories and advance their efforts rather than continue to struggle with baseline concepts.

SARMA offers a grassroots approach to the development of a common lexicon for the profession that is focused on independent and objective standardization of terms, working with a number of corporations, experts, and government agencies to achieve this goal. It is not alone, however - the American Society for Industrial Security (now known as ASIS International) has also launched its own efforts to provide grassroots solutions to this problem. These associations and others like them recognize the need for common terminology in the industry and the costs that are being incurred as a consequence of the lexicon problem not being resolved, and are motivated to work together to solve the problem out of their own interests as practitioners. This has an added benefit for the U.S. Government, which incurs little to no cost for the creation of these standards – one of the reasons that legislation, the NTTAA, was signed into law in early 1996 to encourage government agencies to participate in and accept public voluntary consensus standards.

When a common baseline is achieved for security analysis and risk management, including terminology, lexicon, methodology, and analytical principle, everyone benefits. Training will allow the education of a new generation of analysts, costs for interoperability of analytical results will decrease, and the government will have a standard for comparison as new methodologies come to its attention. Comparable analytical results provide increasing benefits as they rise to higher decision-makers who must make key policy decisions based on comparison of results, and for whom incompatible analysis has serious and long-lasting effects. These benefits help the government and industry as a whole, and will result in a safer and more secure America as policy makers can base judgments on solid, reputable, and understood terminology and compatible methodologies.

Andrew G. Harter currently works as an Analyst for SRA International, Inc., serving as Associate National Agency Coordinator for the Governor's Office of Homeland Security, State of California, where he performs liaison duties between the terrorism centers of California and federal agencies. He is a volunteer for the Security Analysis and Risk Management Association (SARMA), where he is the Team Leader for their Common Lexicon Project.

Prior to employment with SRA, he was an Intelligence Analyst for the Federal Bureau of Investigation, where he helped establish the Risk Assessment Unit of the Foreign Terrorist Tracking Task Force, with specialization in counterterrorism analysis and terrorist risk assessment, training intelligence analysts in analytical methodologies, business processes and work flows, and defining end user technical requirements for analytical software development programs.

He also has experience as Communication Lead and Software Consultant, previously working within the information technology division of an international electric utility. He is a member of International Association of Law Enforcement Intelligence Analysts (IALEIA), and a lifetime member of both the International Association for Counterterrorism and Security Professionals (IACSP) and National Eagle Scout Association (NESA).

---

[1] Delk, James D. Fires & Furies: The L.A. Riots. Palm Springs, Calif.: ETC Publications, 1995, pp. 221-22.
[2] Public Law 104-113, 104th Congress of the United States. http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=104_cong_public_laws&docid=f:publ113.104
[3] Office of Management and Budget, Circular No. A-119 Revised, February 10, 1998. http://www.whitehouse.gov/omb/circulars/a119/a119.html#3
[4] Office of Management and Budget, Circular No. A-119 Revised, February 10, 1998. http://www.whitehouse.gov/omb/circulars/a119/a119.html#3
[5] The order of discussion may vary from the listed order of attributes.
[6] "Wikinomics: How Mass Collaboration Changes Everything." Talk of the Nation Radio Show. National Public Radio. January 2, 2007. http://www.npr.org/templates/story/story.php?storyId=6711038
[7] Bain, Ben. "Diplomats Take a Shine to Wikipedia-like App." FCW.com. July 25, 2007. http://fcw.com/article103315-07-25-07-Web
[8] Shrader, Katherine. "Over 3,600 intelligence professionals tapping into 'Intellipedia.'" Associated Press. USA Today. November 2, 2006. http://www.usatoday.com/tech/news/techinnovations/2006-11-02-intellipedia_x.htm
[9] Marpet, Mark I. "An Ethical Issue in Voluntary-Consensus-Standards Development: A Decision-Science View." Journal of Business Ethics, Vol. 17: 1701-1716, 1998.
[10] Shor, Mikhael, "Pareto Optimal." Dictionary of Game Theory Terms, Game Theory.net. http://www.gametheory.net/dictionary/ParetoOptimal.html. Accessed August 7, 2007.
[11] Marpet, Mark I. "An Ethical Issue in Voluntary-Consensus-Standards Development: A Decision-Science View." Journal of Business Ethics, Vol. 17: 1701-1716, 1998.
[12] Ibid.

The Intangible Value of Security in a Volatile Global Economy*

Robert P. Liscouski and Nir Kossovsky

It is not just bad management that can harm the value of intangible assets; they can be deliberately targeted for both criminal and political reasons.

During the highly contested 1992 elections for the US Presidency, Democratic adviser James Carville realised he had to focus both the electorate and his candidate, Bill Clinton, on what really mattered: "It's the Economy, Stupid."

In our volatile geopolitical environment, the economy of nation-states – most often the United States – is seen by those seeking to bring about political collapse as Carl von Clausewitz's centre of gravity. And in an economy where intangible assets comprise upwards of 80% of the market capitalization of traded companies, the centre of gravity resides somewhere within the value of intellectual properties and other intangibles.

Intangible assets interdependently support a company's enterprise value. This article looks at security as an intangible asset and defines board-level strategies now being examined by the Intangible Asset Finance Society's (IAFS) Security Risk Management Committee that can help companies realise and protect that value.

The von Clausewitzian Centre of Gravity

Carl Phillip Gottfried von Clausewitz (1780-1831) penned the magnum opus On War (1832), one of the two most important Western works ever written on the theory of warfare and strategy. The other is by the Athenian writer Thucydides: The Peloponnesian War (circa 400 BC).

A central metaphore of On War, a text increasingly used in business schools, is the centre of gravity. Its use remains essentially consistent with the concept's representation in the mechanical sciences: "It is against that part of the enemy's forces where they are most concentrated that, if a blow were to occur, the effect would emanate the furthest; furthermore, the greater the mass our own forces possess when they deliver the blow, the more certain we can be of the blow's success."

Striking at or otherwise upsetting the centre of gravity can cause the object to lose its balance or equilibrium and fall to the ground. The US economy is the centre of gravity of the US government and intangible assets are at the heart of the US economy.

SECURITY IS AN INTANGIBLE ASSET

Like reputation, safety and quality, security comprises elements of what is generally known as a brand and interdependently supports other intangibles comprising intellectual properties. Collectively, superior management of security and other intangibles is associated with higher gross margins, net income, earnings multiples, enterprise value and market capitalisation.

In companies spanning a wide range of industries, security risk is recognised as being material to the enterprise. Table 1 shows a sample of companies across all of the major US trading exchanges disclosing in their 2006 annual reports risks from terrorism. That such

risks are disclosed in filings to the US Securities and Exchange Commission indicates that company boards recognise the materiality of these risks and, as such, accept that it is a board level responsibility to oversee management of these risks.

Ticker	Name	Market	Business
SMTC	SEMTECH CORP	NasdaqGM	Semiconductor – integrated
MPR	MET PRO CP	NYSE	Diversified machinery
DEBS	DEB SHOPS INC	NasdaqGS	Apparel stores
TAG	TAG IT PACIFIC INC	AMEX	Textile – apparel clothing
SAI	SAIC INC	NYSE	Technical services
ARSD.OB	ARABIAN AMER DEV CO	OTC BB	Oil & gas refining & marketing
PVH	PHILLIPS VAN HEUSEN	NYSE	Textile – apparel clothing
JCP	PENNEY J C CO HOLDIN	NYSE	Department stores

Table 1. Companies disclosing in their 10-K SEC filing a material security risk

SECURITY PERILS ARE NOT INTANGIBLE

Since 2001, US businesses and other icons have increasingly become the primary focus, as enemies of the state have shifted their targets from assets owned by the government to assets owned by the private business sector with the goal of maximising enterprise damage. And consistent with the economic focus, an increasingly larger share of the known US targets are in the financial sector.

Security perils are not limited to nonstate actors (terrorists). State sponsored sources of peril, organised crime groups, extortionists and common criminals can all find value in destroying, or threatening to destroy, the intangible asset value of a business or industry sector. Table 2 summarises recent publicly disclosed terror threats and attacks, not only on US businesses and icons but also those from other western countries.

Target	Year(s)	Actor
Achille Lauro – (target was cruise ship with American passengers)	1985	Palestine Liberation Organisation
Pam Am 103 (target was "US airlines" of which Pan Am was most iconic)	1987	Libya – state sponsor
McDonald's as an iconic US business in Europe and other parts of the world	Frequent target since the 1980s	Various nationalist, ecological and far left inspired organisations
World Trade Center, New York City	1992	Al Qaeda
World Trade Center, New York City	2001	Al Qaeda
CitiGroup Buildings, New York City	Summer 2004	Al Qaeda Threat
Wall Street/NY Stock Exchange	Summer 2004	Al Qaeda Threat
Prudential Insurance Company	Summer 2004	Al Qaeda Threat
BP in Colombia	Current	Regional terrorist organisations
Shell Nigeria and Algeria	Current	Regional terrorist organisations
Mobil Nigeria and Algeria	Current	Regional terrorist organisations

Table 2. Recent attacks and threats to enterprise value

GOOD SECURITY RISK MANAGEMENT PRACTICES

The Security Risk Management Committee of the IAFS has been evolving corporate governance standards for intangible asset management based, in part, on a risk analysis model initially developed at the US Department of Homeland Security. The first of two central tenets of this model is that risk arises from the difference between threat capability/probability and precautionary capability/effectiveness (Figure 1).

Figures 1a & 1b

Risk arises from the difference between threat capability/probability and precautionary capability/effectiveness (1a). This implies that an optimal level of security product deployments and security process implementations is relative and that acute changes in either the threat or precautionary capabilities create periods of maximum relative risk (1b)

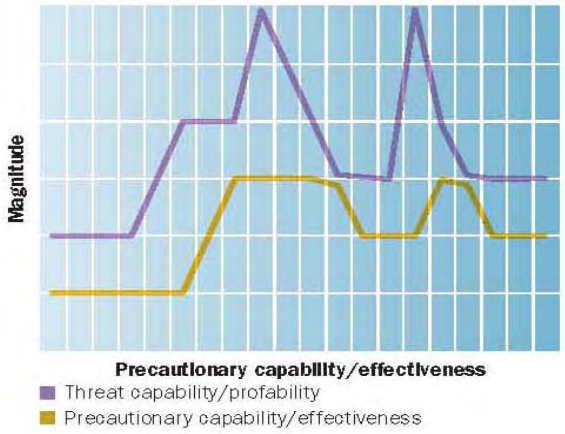


Figure 1a. Time series of threat and capability volatility

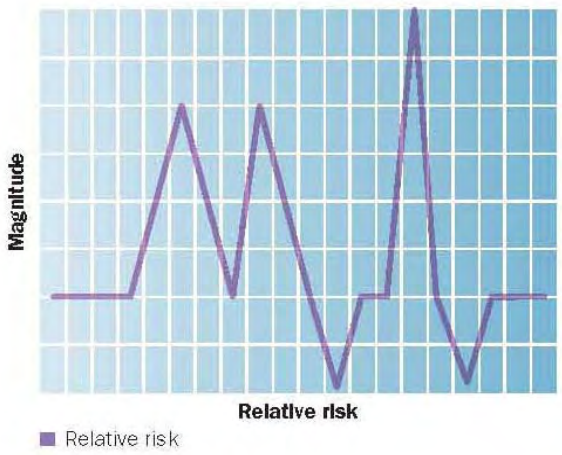


Figure 1b. Time series of relative risk

This model implies that an optimal level of security product deployments and security process implementations is relative, and that acute changes in either the threat or precautionary capabilities create periods of maximum relative risk. For example, Figure 2 shows that the capital markets recognised the rise in relative risk associated with US-based hotel chains following the 11th September 2001 attack on the World Trade Center.

Figure 2

The interplay between security and stock price volatility. Note the rise in beta of an index of US corporate hotel businesses over the past few years as high profile security events have increased concerns about the sector's economic security.

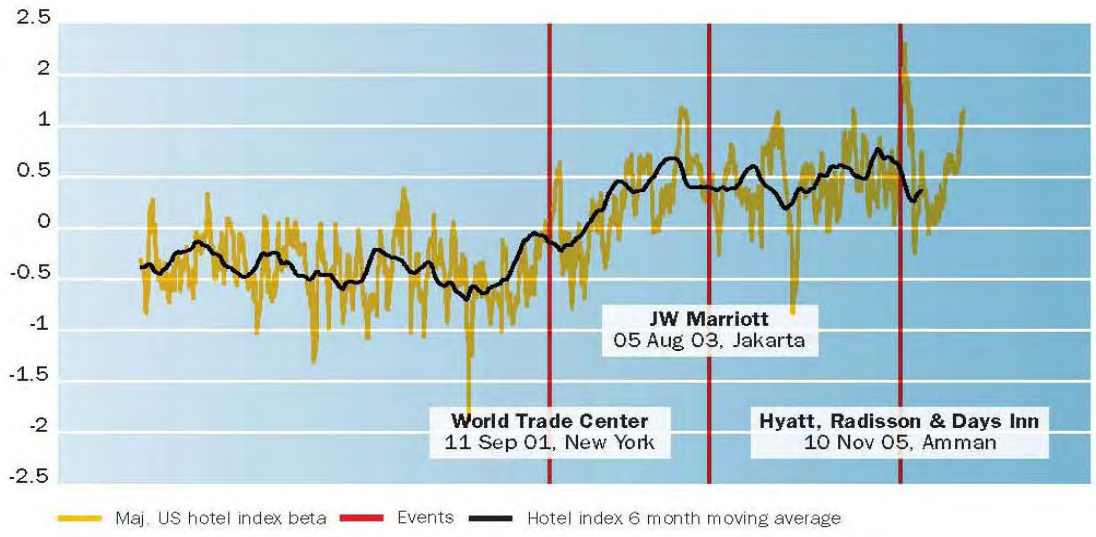


Figure 2. Hotel index beta relative to S&P 500

The second tenet is that events will nevertheless occur. In such instances, recovering, reconstructing and or reconstituting the lost intangible assets – resilience in security parlance – will determine whether the impairment is ultimately fatal or merely disruptive.

Insurances can provide capital to support a good practice for optimising resilience in companies where corporate controls at the board level have paved the way for the adoption of a robust intangible asset management philosophy, and the establishment of highly protected risks (within the insurance industry, Highly Protected Risk (HPR) is a status awarded when the insured object meets higher standards in order to obtain significantly lower premiums. Protections relate to conformance with good risk management practices and best practice standards).

A FRAMEWORK FOR GOOD SECURITY RISK MANAGEMENT PRACTICES

Operationally, the primary challenge for those tasked with preserving enterprise value by maximising resilience – the corporate board – is setting targets for management. There are no standards for what is secure enough, no meaningful actuarial measure of threat and no framework for reasonableness of capital investment. In fact, the only certain fact is that security events, or threats of security events, can be catastrophic in terms of enterprise value.

We suggest a process comprising five steps, that similar to good manufacturing practices and other process standards, can not guarantee a good outcome but can improve the probabilities:

- Identifying the priorities.
- Managing risk in a dynamic and ambiguous threat environment.
- Ensuring commitment.
- Making the business case.
- Battling complacency.

Priorities

In every industry, certain aspects of its operations provide all stakeholders with assurances that the goods and services delivered will meet quality standards. In the food industry it is freedom from contaminants, toxins and poisons. Thus, the Tylenol poisoning (criminal), the Taco Bell and spinach E. Coli scares (accident) and the current scare over pet food contamination (culprits, if any, undetermined at this time) all represent central intangible priorities where security threats may manifest. In the travel industry, it is a combination of health (cruise line Norwalk virus matter), customer service (Jet Blue IT systems collapse) or the most basic freedom from assault (cruise line Achille Lauro). Identifying the areas where an attack will cause maximum damage to enterprise value (the centre of gravity) is the first step in good security intangible asset risk management practice. Building resilience into the business to protect against enterprise value loss following an attack includes both the repair of people, products and processes impaired by an attack, as well as devising a world class communications plan resulting in sustainable market and consumer confidence in the company's ongoing ability to deliver its products and honour its financial obligations.

Managing Risk in a Dynamic and Ambiguous Threat Environment

Recognising that risk is relative, as illustrated in Figure 1, a and b, good risk management practices call for a rich understanding of the baseline geopolitical and criminal threat environment as those threats relate to the companies vulnerabilities. This involves the constant flow of information to senior decision makers regarding evolving threat conditions; and accurate identification and assessment of an entity's baseline security measures and vulnerabilities. In our practice, we tend to segment

businesses by industry category and organisations on the basis of people processes, physical measures and cyber measures.

Organisational Commitment

As with other matters that speak to enterprise value, an organisation must engage its leadership at the highest level, i.e., board and C-level leadership. Within this leadership, two cultural values must flow through the organisation:

- A culture of communication. Those at the tactical level closest to threat data must understand that they are empowered to question security assumptions.

- A culture of action. There is never enough or proper information and those empowered to act need to be willing and able to act on the basis of information available. As Clausewitz noted: "It is even better to act quickly and err than to hesitate until the time of action is past."

Initial and Ongoing Investments

The business case for risk mitigation and insurances to protect enterprise value against catastrophic security risk may not conform to a conventional ROI analysis. On the other hand, in the absence of reasonable efforts, liability falls squarely on those charged with corporate governance, affirming the principle that catastrophic risk management is a core strategic concern.

Two aspects of good intangible asset risk management practices warrant repeating:

- Monitor and establish procedures to reduce vulnerabilities above the baseline as the threat changes.

- Seek insurances and other efficient risk transfer instruments to cover the costs arising from implementation of a plan leading to resilience.

Battling Complacency

The absence of an event may lead to a lack of focus and appreciation of the magnitude of the security perils to intangible asset and therefore enterprise value. Financial pressures may lead to a questioning of the ongoing wisdom of sustained investments. The single most effective means of combating complacency is to conform to good practices and ensure the periodic board-level examination of the risk management processes (Figure 3).

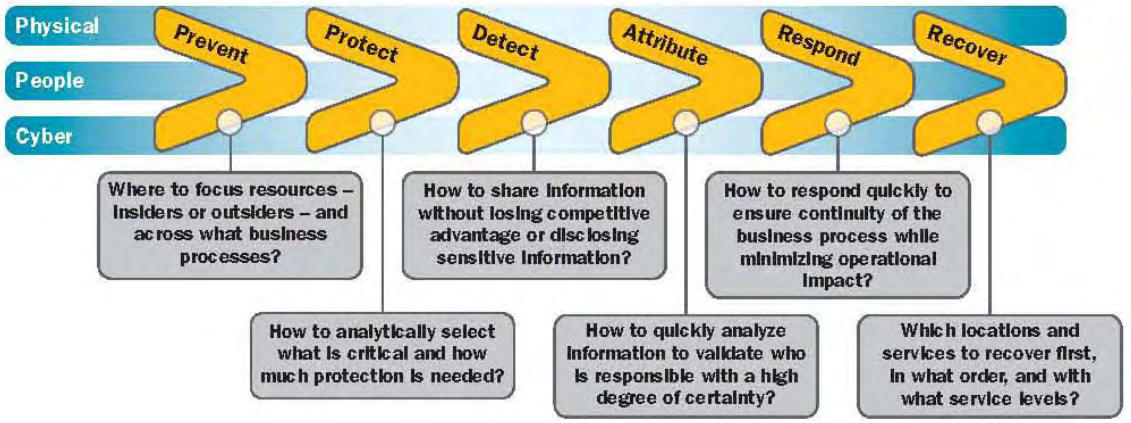


Figure 3. Questions for a board of directors, the answers to which would be part of a company-specific intangible asset management standard

GOOD SECURITY RISK MANAGEMENT STANDARDS

The IAFS's Security Risk Management Committee recognises that security issues are historic matters of corporate concern and much work has been done by industry, associations and certain government agencies such as the Department of Homeland Security in the US, to craft guidelines for different operational risks. The Committee recognises that industry knows best how to govern its processes and will draw upon these sources, and others, to craft an integrated standard that defines standards at the corporate governance level. Exemplary resources include general guidelines useful across many industries and sector-specific guidelines from industries that tend to be closely regulated (Table 3).

The board of directors oversees management and the audit committee oversees financial controls that include asset utilization and protection. The IAFS's Security Risk Management Committee believes it is critical that the board and senior company management abandon the historical notion that security relates to guns, gates and guards, and adopts a comprehensive approach to protecting its brand and intangible assets. The changing risk environment demands forward thinking on this topic as many past incidents have demonstrated that the

Table 3: Exemplary source materials for crafting intangible asset management standards relating to security and enterprise value

Selected cross industry best practices/guidelines:

- ISO17799 Code of Practice for Cyber Security.
- ISO13335 Risk Management Controls.
- ISO15408 Common Criteria.
- NFPA1600 Standards for Physical Safety.
- ASIS Security Guidelines for Homeland Security.

Selected sector-specific best practices/guidelines:

- Responsible Care Standards (chemical).
- NERC1200 (energy).
- FFIEC Handbook for Audit (financial services).
- AAR Class I Freight Guidelines (transportation).
- American Lifeline Alliance Standards (oil & gas).
- FTA Emergency Preparedness (transportation).

intangibles are now perceived as the centre of gravity.

In most traded companies, the buck stops with the CEO and the board of directors. In companies where intangible assets comprise a material fraction of the market capitalisation, shareholders reasonably expect that the company will have in place systems to ensure the optimal management of those assets and resilience should those assets be impaired. Security triggers are one source of catastrophic perils.

Controls and related processes can be reflected in good practice standards and can reduce the variance associated with asset management. The Intangible Asset Finance Society's Security Risk Management Committee invites comments and participation as it labours to promulgate IAM standards. As James Carville might say today: "It's the intangibles, stupid."

Robert P. Liscouski is an executive-in-residence with Centurion Holdings, LLC, New York, and chairs the Intangible Asset Finance Society's Security Risk Management Committee. He is the former Assistant Secretary for Infrastructure Protection, US Department of Homeland Security.

Nir Kossovsky, MD is the CEO of Steel City Re, LLC, an enterprise value assurance company headquartered in Pittsburgh, and also serves as the Executive Secretary of the Intangible Asset Finance Society.

* A version of this article first appeared in Issue 24 of Intellectual Asset Management/IAM magazine, June/July 2007. IAM magazine (www.iam-magazine.com) is published by Globe White Page Ltd.

This monograph was compiled by Liz Jackson of the Critical Infrastructure Protection Program, George Mason University School of Law. Please forward any questions or comments to:

Liz Jackson, Senior Associate, Special Projects
ejackso4@gmu.edu

Critical Infrastructure Protection Program Resources

In addition to project information and research products posted on the Critical Infrastructure Protection (CIP) Program's website (http://cipp.gmu.edu/), the Program offers two resources for critical infrastructure-related information. The first, *The CIP Report*, is the CIP Program's monthly newsletter. The second, the CIP Library, is an online repository of information about critical infrastructure protection and other topics of interest.

The CIP Report

As part of its outreach efforts, and in order to maintain awareness about critical infrastructure, the CIP Program generates a monthly newsletter (*The CIP Report*) that is read by innumerable stakeholders from the public and private sectors, academia, international organizations, and other entities concerned with critical infrastructure. The inaugural issue of *The CIP Report* was released in July 2002, and all issues of *The CIP Report* are publicly available in *The CIP Report* Archive (http://cipp.gmu.edu/report/cip_reportarch.php).

The CIP Report typically includes interviews with high-level government officials or private sector executives, background pieces on select topics, and articles by CIP Program staff discussing a range of timely issues and Program research projects. The theme of each issue varies and regularly addresses topics of current discussion in the homeland security arena. Numerous critical infrastructure and key resource (CI/KR) sectors have been covered by *The CIP Report*. The past few years, a dedicated issue has been released on international critical infrastructure protection, featuring interviews and articles from contributors around the globe. Issues have also focused on research and training.

Through *The CIP Report*, the CIP Program facilitates discussion of key topics and informs readers of valuable information concerning the field of critical infrastructure protection. The Program also continually engages readers to elicit feedback, providing insight into current topics of discussion in the critical infrastructure community for future issues.

CIP Library

The CIP Library (http://cipp.gmu.edu/clib/) features numerous webpages housing a wealth of information about critical infrastructure protection, as well as topics such as infrastructure recovery and restoration. These webpages include:

- Bibliography of CIP Program-Sponsored Research Publications;
- Summary of CIP Program-Sponsored Projects;
- CIP Digital Archive;
- Selective Government Reports on Infrastructure Protection;
- Selective Reports on Critical Infrastructure Recovery and Restoration;
- Selective Government Reports on Hurricanes; and
- Selective International Reports and Other Documents.

The first two webpages feature abstracts of CIP Program-sponsored works. The contents of the remaining webpages include government reports and directives; congressional reports, hearing transcripts, and legislation; publications of notable non-government organizations; and other relevant documents and weblinks. A synopsis of each webpage is found on the CIP Library's main page. The CIP Library is frequently updated with new information to ensure users remain well-informed on this important subject matter.