



Security Analysis and Risk Management Association

JOIN SARMA

CONTACT SARMA

## The Risk Communicator: January/February 2008 Edition

Welcome to the Risk Communicator, SARMA's newsletter for information, trends and issues of concern to security analysis and risk management professionals. This complimentary news service is distributed every other month. Please feel free to share this e-mail with your colleagues and encourage them to sign up to get their own copy [here](#).

If your server is blocking HTML e-mails you can view the current Risk Communicator by pasting the following address into your browser:  
<http://sarma.org/news/theriskcommunicato/default.htm>

[Printer Friendly](#)


## SARMA Feature Article

### 9/11 Tragedy Provides Impetus for a Risk Management Success



Port Authority Assets

For John Paczkowski and the rest of the staff at the Port Authority of New York and New Jersey (PANYNJ), the attacks of September 11th were more than just a national tragedy -- they felt like a direct hit. PANYNJ was the owner of the World Trade Center (WTC) complex, and 84 staffers, including the executive director and head of its public safety office, had been killed in the attack. "The agency suffered a real body blow," recalls Paczkowski, then and now the director of emergency management and security at PANYNJ.

In the wake of the disaster, the agency realized it had a lot of work to do, not just in reconstituting its physical infrastructure and personnel, but also in reviewing its own security and risk management procedures for the airports, bridges, tunnels, ports and buildings under its control. After the 1993 attack on the WTC, officials had undertaken what they thought was a comprehensive security analysis, but the result was mainly more cameras and fences. The 9/11 attacks demonstrated the need for an altogether different approach.

"They were following best practices," Paczkowski says, "but they weren't evaluating relative risk and setting priorities." Not that this would have been an easy task even under the best of circumstances: a post-9/11 review of security needs soon resulted in 23 individual reports with 1,100 specific recommendations and an estimated price tag of more than \$1 billion. This was not manageable, in part because, as a bi-state agency, PANYNJ had a hard time getting the political support to obtain federal funding, and senior officials were beginning to realize that they lacked the ability to make business-like decisions about which security needs to fulfill.

But if PANYNJ officials couldn't rely on the federal government for funding, they hoped at least to get some help developing better risk assessment capabilities. Waiting to assist them was the Office for Domestic Preparedness (ODP) at the US Department of Justice (DoJ), which was already looking for an opportunity to develop a risk assessment template it could offer to similar agencies around the country. Together, PANYNJ and DoJ called in a private company to create a facilitated process by which an agency could look at all of its assets, provide relative risk scores for each of them, manage the inevitable disputes and disagreements among stakeholders, and provide a method for future program evaluation.

"What is absolutely unique is that they developed a risk assessment process that made dissimilar assets comparable, which in turn allowed PANYNJ to develop a justifiable plan for prioritizing their security investments across the agency," says Kerry Thomas, who helped run the DoJ program. Known as the Special Needs Jurisdiction Toolkit, the approach relied on a series of assumptions of relative risk developed by a multidisciplinary team of engineers and counter-terrorism experts. Using these baseline assumptions, the working group performed a three-step process: undertaking a "consequence screen" to rank a series of worst-to-best-case scenarios across PANYNJ's asset base; teasing out the Port Authority's most critical vulnerabilities; and, finally, looking at existing response and mitigation capabilities.

The idea, says Thomas, was to figure out what security countermeasures would have the greatest impact for the dollars invested, and to force competing offices within the Port Authority to "level" their risks and make frank and honest assessments of their needs. In the end, the team came up with a \$500-million, five-year plan for PANYNJ that agency leaders could justify on cost-benefit grounds. Every two years an agency-wide review is performed to gauge risk reduction and make appropriate adjustments based on improved knowledge and technologies, and the payoffs are obvious. "We can take the same infrastructure and attack scenarios, look at the delta, plot the data on a graph, and then re-run the model," says Paczkowski.

These biannual reviews are perhaps the most critical element of the entire Toolkit. Not only does

#### Contents

- [SARMA Feature Article](#)
- [Reports and Reviews](#)
- [Officers' Corner](#)
- [Conferences and Training](#)
- [Miscellaneous](#)
- [Links of Interest](#)

#### Subscriptions

[Subscribe](#)  
[Unsubscribe](#)

to the Risk Communicator

#### Contact SARMA

**SARMA**  
 P.O. Box 710172  
 Herndon, VA 20171  
 Phone: (703) 635-7906  
 Fax: (703) 635-7935  
 E-mail: [info@sarma.org](mailto:info@sarma.org)

#### Get Involved in SARMA

Get involved with SARMA today.

[SARMA website](#)  
[SARMApedia](#)  
[Volunteer To Serve](#)  
[Feedback / Input Form](#)  
[Join SARMA](#)

#### Sponsor Notices

SARMA thanks the following organizations for their support:



QinetiQ North America



CRITICAL INFRASTRUCTURE PROTECTION PROGRAM

standardization make it possible to track improvement over time, but new information -- either about the vulnerability of a piece of infrastructure or about the nature of the threat -- can be incorporated to provide the freshest understanding possible. The first risk assessment using the Toolkit, for instance, did not include data on the Port Authority's downtown tunnels, which were closed after 9/11. When they were included two years later the risk profile for the office responsible increased. This didn't indicate failure; it simply meant that the overall picture had come into sharper focus, thus allowing an enhanced response (which in turn would be measured at the next review). Likewise, a well-publicized threat in 2006 against the PATH train system increased that system's profile as well, a sign that the process was flexible enough to react to a changing environment.

Most of the time, however, the process has resulted in improved -- that is to say, decreased -- risk profiles for the Port Authority's assets. In one case, a blast analysis of the agency's bridges and tunnels led to a comprehensive target-hardening effort, which "resulted in a tremendous improvement in terms of relative vulnerability," Paczkowski says. Improvement can also be seen in the renewed confidence among the agency's managers that decisions are being based on hard numbers and not emotion or rent-seeking. Indeed, Paczkowski is impressed by the level of collegiality among competing offices. Although it required a significant amount of work up front to create the baseline risk assumptions, he says, the payoff was that no office could game the system by exaggerating its own needs. Each time an office made claims that strayed from those original assumptions, it would have to justify them to the multi-disciplinary committee.

The results have far outpaced expectations and raised the bar for security professionals nationwide. It may even provide a success story the federal government could emulate. Since its initial development and application at PANYNJ, at least 35 additional transit agencies have used the Toolkit. "Any agency contemplating using the Toolkit would want to know if it works," says Paczkowski. "My answer is an unequivocal yes."

*Avi Klein, a Washington DC-based freelance writer specializing in defense issues, is a frequent contributor to the Washington Monthly and previously served as senior writer at Homeland Security Daily Wire. He can be reached at [avi.klein@mac.com](mailto:avi.klein@mac.com).*

## Risk Analysis Career Training for Disabled US Servicemen

*A Partnership between SARMA and Hire Heroes USA*

Disabled American veterans returning home from overseas conflicts and hoping to embark on careers in security analysis and risk management will soon have a new resource to help them turn that hope into reality.

SARMA has reached a cooperative agreement with Hire Heroes USA (HHUSA), a non-profit career placement agency, to develop a customized Career Training Program (CTP) for vets with service-related disabilities. HHUSA acts as a bridge, matching employment opportunities at participating companies with the veterans' career interests and skill-sets.

Under the agreement, SARMA will develop a series of security analysis and risk management-focused training and mentoring sessions, drawing on its security expertise and knowledge of government and private-sector requirements. The CTP will be offered at no charge to participating HHUSA veterans.

In addition to traditional classroom learning, SARMA will adapt the training sessions to the physical needs and geographical circumstances of disabled veterans through the use of online learning tools. In this way, veterans still undergoing medical treatment and physical therapy will be afforded the same opportunity to learn as those without disabilities.

Hire Heroes USA representatives will also be featured speakers and exhibitors at SARMA's National Conference on Security Analysis and Risk Management, to be held from 13-15 May in Arlington, VA. Corporations and government agencies interested in participating in the program should contact Bayne Tippins at [btippins@hireheroesusa.org](mailto:btippins@hireheroesusa.org). [[Learn More About Hire Heroes USA](#)]

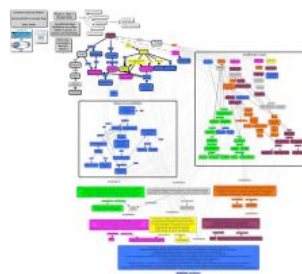
## Cracking the Lexicon Code

*How (and Why) SARMA is Developing a Common Vocabulary for Security and Risk*

When two risk experts sit down to discuss some aspect of their craft, chances are they will start off with a healthy exchange of ideas. But as dialogue turns into debate, it will almost invariably bog down amid growing misunderstanding and confusion. By the time the "discussion" wraps up, these individuals will in effect have hardly communicated at all.

An outsider might be tempted to conclude that the experts must be speaking two different languages -- and in fact that would not be far from the truth. What causes the misunderstanding, however, is not their lack of English comprehension; it's that their vocabularies are incompatible. For example, they might use the same word to describe two entirely different objects, or perhaps they each will employ a different term to describe the identical concept.

If such a fundamental disconnect can occur at the level of a single conversation, it's not hard to imagine how the misunderstandings and confusion will be magnified when the dialogue is at an intra-agency or inter-departmental level, nor is it difficult to imagine the consequences when what's at stake is the security of the nation.



Click to Enlarge Concept map for "Asset"



### Links of Interest

[SARMApedia](#)

[Hire Heroes USA](#)

### The Risk Communicator

*The Risk Communicator, newsletter of SARMA, the Security Analysis and Risk Management Association*

Send questions and comments to  
Editor-in-Chief  
[newsletter@sarma.org](mailto:newsletter@sarma.org)

Copyright 2008.  
SARMA All rights reserved.

### [PRIVACY POLICY](#)

The views expressed in the Risk Communicator reflect the views of their authors, and do not necessarily reflect the views of SARMA, the US Government, or the employers or clients of the contributors.

Untangling this linguistic mess was one of the driving forces behind the establishment of SARMA in May 2006, leading to the creation of a mechanism whereby the multiple vocabularies -- or lexicons -- of security and risk could be collected, analyzed and reconciled in an open and unbiased manner through broad consensus. This mechanism is called the Common Lexicon Project, and it is one of the core elements of the broader common knowledge base now known as SARMApedia.

Over the past two years, many individuals have generously contributed their time and expertise to Phase I of the Common Lexicon Project, helping SARMA to amass an extensive glossary of terms commonly used by the security analysis and risk management profession. Not surprisingly, given the scenario described above, the typical term contains multiple -- and sometimes conflicting -- definitions (see the [SARMApedia](#) for examples).

As SARMA enters its third year, it is embarking on Phase II of the Common Lexicon Project, which starts the process of analyzing and reconciling competing definitions. This will be followed by Phase III, the final stage, for which the goal is to arrive at a single broadly accepted definition for each term. It is important to note that the three phases will be continuously revisited in an ongoing cycle, since there will always be new definitions emerging, which must then be analyzed against and reconciled with the existing lexicon.

To aid the process of linguistic analysis and consensus building in Phases II and III, SARMA plans to employ a methodology known as concept mapping. Graphical tools for organizing and representing knowledge, concept maps allow the user to break a definition down into its component parts and to highlight the relationships and links between each part. When multiple definitions are involved, concept mapping can be used to merge redundant elements and bring core concepts to the forefront, among its many other features. Since experts contributing to the Common Lexicon Project are geographically dispersed, moreover, SARMA is considering the use of a web-based version known as CmapTools, originally developed by the Institute for Human and Machine Cognition and adapted for the Common Lexicon Project by [Perigean Technologies](#).

On the Definitions page of SARMApedia, by way of example, the term "Asset" contains seven distinct definitions gleaned from multiple sources. The accompanying graphic depicts the term after it has been keyed into the Cmap tool but before the consolidation and merger process has taken place. The entire map can be laid out automatically to provide a structured view of all the merged concepts and their original links or it can be filtered to depict only the most critical elements. In the case of "Asset", the most prevalent concepts and links will move toward the center of the screen, while the subcategories and less prevalent elements will shift to the sides. With such visual clarity, a group of experts can make better decisions about which elements of the term are essential and which are ancillary, thereby arriving at a consensus definition in the most efficient way.

As mundane as it may seem, creating a commonly accepted vocabulary is a critical first step in the pursuit of common standards for any professional community. It is essential, moreover, that this process take place in a completely transparent, unbiased and collaborative environment. The historical record of common lexicon initiatives is littered with attempts by one organization or another to impose its narrow definitions on the community as a whole, often developed behind closed doors with little consultation or expert input. In no case did this approach ever succeed in producing a vocabulary everyone was willing to use.

Without a Common Lexicon for the security analysis and risk management profession, it also will be a challenge for SARMA to make significant headway in its other key goals: the standardization of security and risk assessment methods, and the establishment of Generally Accepted Risk Assessment Principles (GARAP). These three elements represent the foundation and building blocks of a structure that will serve and sustain the profession well into the future.

It's time to get to work.

-----  
 Editor's Note: The SARMA Common Lexicon Project team is preparing a presentation on the concept mapping process at the SARMA conference in May, and is interested in hearing from volunteers who may wish to take part in the process over the next 12 months. For more information, please contact Common Lexicon Committee Chairperson Andrew Harter at [andrewgharter@yahoo.com](mailto:andrewgharter@yahoo.com).

[Return to the top](#)

## Reports and Reviews

### Critical Infrastructure Protection: Elements of Risk



Prepared by the George Mason University's Critical Infrastructure Program, this monograph contains seven papers that "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." SARMA President Ed Jopeck and Vice President Kerry Thomas contributed the lead article. [\[Click Here to View the Monograph\]](#)

### Annual Threat Assessment of the Director of National Intelligence

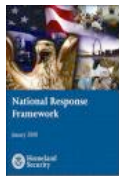
On 5 February 2008, J. Michael McConnell, the Director of National Intelligence (DNI), presented his Annual Threat Assessment before the US Senate Select Committee on Intelligence. In the testimony, the DNI focused his comments on the following issues:



- The continuing global terrorist threat, but also the setbacks the violent extremist networks are experiencing;
- The significant gains in Iraqi security since this time last year and the developing political and economic improvements;
- The continuing challenges facing us in Afghanistan and in Pakistan, where many of our most important interests intersect;
- The persistent threat of WMD-related proliferation;
- The vulnerabilities of the US information infrastructure to increasing cyber attacks by foreign governments, nonstate actors and criminal elements;
- The growing foreign interest in counterspace programs that could threaten critical US military and intelligence capabilities;
- Issues of political stability and of national and regional conflict in Europe, the Horn of Africa, the Middle East, and Eurasia;
- Growing humanitarian concerns stemming from the rise in food and energy prices for poorer states;
- Concerns about the financial capabilities of Russia, China, and OPEC countries and the potential use of their market access to exert financial leverage to achieve political ends.

[\[Get the Report\]](#)

### National Response Framework: January 2008



Replacing the National Response Plan, "This National Response Framework (NRF) [or Framework] is a guide to how the Nation conducts all-hazards response. It is built upon scalable, flexible, and adaptable coordinating structures to align key roles and responsibilities across the Nation. It describes specific authorities and best practices for managing incidents that range from the serious but purely local, to large-scale terrorist attacks or catastrophic natural disasters. This document explains the common discipline and structures that have been exercised and matured at the local, tribal, State, and national levels over time. It describes key lessons learned from Hurricanes Katrina and Rita, focusing particularly on how the Federal Government is organized to support communities and states in catastrophic incidents. Most importantly, it builds upon the National Incident Management System (NIMS), which provides a consistent template for managing incidents. [\[Get the Document\]](#)

[Return to the top](#)

## Officers' Corner

### SARMA's 2007 Financial Report



SARMA Treasurer Dave Brown summarizes the Association's 2007 financial picture.

In summary, SARMA had an excellent financial year in 2007 generating enough revenue to pay off all start-up costs and outstanding debts. Total income for 2007 was \$40,232.50. Total expenses were \$21,655.26, leaving SARMA \$20,988.33 in available funds at the close of the year. Additionally, SARMA was approved by the IRS as a non-profit professional organization. [\[Get the Report\]](#)

[Return to the top](#)

## Conferences and Training



Hosted by: **SARMA** (Security Analysis and Risk Management Association), **GEORGE MASON UNIVERSITY** School of Law, **CRITICAL INFRASTRUCTURE PROTECTION PROGRAM**

Sponsored by: **PRICEWATERHOUSECOOPERS**, **Booz | Allen | Hamilton** (delivering results that endure), **SRA INTERNATIONAL, INC.**, **CYBRINTH**, **duostech**

Special Guest: **HIRE HEROES USA**

Registration is now open for the National Conference on Security Analysis and Risk Management being

held 13-15 May 2008 in Arlington, VA. This year's conference will be co-hosted with George Mason University's Critical Infrastructure Protection Program. The keynote speaker will be Joel Bagnol, Deputy Assistant to the President for Homeland Security and Acting Homeland Security Advisor. To register or learn more, visit the conference site at <http://sarma.org/events/conference/>. If you are interested in presenting at this conference, please follow the instructions at the Call for Speakers on the SARMA web site. [[View Conference Information](#)]

#### Defense Industrial Base/Critical Infrastructure Protection Conference and Technology Exhibition

7-9 April 2008, Hyatt Regency, Miami, FL. The Conference and Expo will enable federal, state, and local governments, and members of the defense industrial base to collaborate, and share information related to the challenges and procedures for ensuring various aspects of defense industrial base mission assurance in an all-hazards environment. [[Go to Conference Website](#)]

#### National OPSEC Conference

7-11 April in Denver, CO. SARMA representatives will be among the speakers at this upcoming event. [[Go to Conference Website](#)]

#### Critical Infrastructure Protection Workshop

5-7 June at the Naval Postgraduate School in Monterey, CA. Entitled "Critical Infrastructure Protection: Metrics and Tools," this workshop is being organized by the Center for Homeland Defense and Security, and the Center for Contemporary Conflict. [[Go to Conference Website](#)]

[Return to the top](#)

## *Miscellaneous*

#### Want to Contribute to the Risk Communicator?

Do you know of an item you would like to see included in the Risk Communicator? Do you have ideas for new and interesting features for future editions? If so, please contact the newsletter staff at [newsletter@sarma.org](mailto:newsletter@sarma.org).

[Return to the top](#)