



Security Analysis and Risk Management Association

JOIN SARMA  
CONTACT SARMA

[Printer Friendly](#)

## The Risk Communicator: August-September 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/theriskcommunicato2/>

## Officers' Corner

### Letter from Kerry Thomas, SARMA's New President



*Kerry Thomas*

As many of you know, SARMA held elections for its Board of Directors earlier this year. The new Board has now fulfilled its responsibility to elect officers, and I was fortunate enough to be chosen to succeed Ed Jopeak as the Association's next President.

Having served for the past year as SARMA's Executive Vice President, I am extremely excited about the opportunity to assume a new role and deeply honored by the trust this represents on the part of the Board of Directors and our members.

I will also have a great team to work with, and I would ask that you join me in congratulating our other newly elected or re-elected officers: John Paczkowski (Executive Vice President), Ken Knox (Secretary), and Dave Brown (Treasurer). In addition, the terms of two other officers do not expire until next year, and both John Boatman (Vice President for Operations) and Nancy Renfroe (Vice President for Projects) will continue to serve in these respective capacities. Concurrently, Ed will move into the newly created position of Immediate Past President, where he will assist me with the transition and continue to serve as a strategic advisor and ombudsman for the Association.

As SARMA enters its third full year of existence, we have a great many things to be proud of. Thanks in large measure to the hard work of Ed and a small

### Contents

- [Officers' Corner](#)
- [News](#)
- [Commentary](#)
- [Key Reports and Reviews](#)
- [Students' 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](#)

group of dedicated volunteers, SARMA has already had an impact well beyond that of most fledgling organizations. Some of our successes include:

**+ Establishment of the Common Knowledge Base Project** designed to begin tackling the substantive issues currently impeding the further maturation of our profession -- the lack of a common professional language, the lack of any consolidated source of information about the profession, and the lack of training or standards for security risk management;

**+ The opportunity to advise both Congress and the White House** on these matters;

**+ Two highly successful national conferences** that have further burnished SARMA's reputation and contributed to its growth; and

**+ The establishment of meaningful relationships with our colleagues in other nations**, including a formal Memorandum of Agreement affiliating SARMA with the Risk Management Institution of Australasia (RMIA).

I look forward to building on these successes and working with Ed, the other officers, the Board of Directors and our members to build on this strong foundation.

In that regard, I have worked closely with my colleagues on the Board over the past several months to identify several interrelated areas where I believe we need to focus our energies in the coming year. I'd like to take a moment to describe these issues, and share why I think they are important to SARMA's future and how I hope to impact them:

**+ Establishing a strategic vision for SARMA's future.** The successes of the past several years present the Association with many exciting opportunities to shape and influence the future of our profession. However, with this promise also comes the risk of losing focus by trying to do too many things at once. To guard against this, we must carefully consider where and how we concentrate our energies and limited resources. The recent establishment of a Strategic Planning Committee is an important first step, and I look forward to working with the Chair and members of the Committee in the coming weeks and months to both define what this future should look like and how we should mold our organization to support that vision.

**+ Developing a long-term funding model.** One of the challenges that will increasingly affect our ability to grow and mature further as an organization is an over-reliance on a few generous corporate sponsors. We must change this. Part of the answer lies with our evolving strategic vision. The other part is, of course, actual marketing and outreach -- communicating the value proposition of supporting SARMA. One way I believe we can address this is by fully staffing our Membership and Outreach Committee, and I will be working with the Vice President for Operations to identify qualified candidates that can help energize this effort.

**+ Obtaining professional association management support.** Another challenge we face is our need to rely on a few dedicated volunteers to manage the daily business of the Association. Tasks such as maintaining our website, communicating regularly with members, issuing the newsletter and planning for the annual conference seem straightforward, but in fact they require a

[Join SARMA](#)

#### Sponsor Notices

SARMA thanks the following organizations for their support:

[Edit](#) | [Hide](#) | [Del](#)



[Edit](#) | [Hide](#) | [Del](#)



[Edit](#) | [Hide](#) | [Del](#)



[Edit](#) | [Hide](#) | [Del](#)



[Edit](#) | [Hide](#) | [Del](#)



Click to  
Insert  
an Ad

#### Links of Interest

#### 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

Copyright 2008.

**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.

substantial investment of volunteer time. While we have managed admirably to date, continued reliance on these volunteers is not a sustainable model for the long term. The Board has discussed a number of potential solutions over the course of the past year, and continues to actively pursue this issue. I will continue to work closely with the Vice President for Operations and our colleagues on the Board to find an answer that both addresses our needs in this area and is affordable in the near term.

**+ Fully resourcing the Common Knowledge Base Program.** The Common Knowledge Base (CKB) represents one of SARMA's principal contributions to the profession. The CKB Program was designed from the outset to address a fundamental set of problems limiting the maturation of the profession. While progress has been made on several of the individual components of the CKB Program, much work remains. Therefore, I plan to work closely with the Vice President for Projects over the coming months to identify areas of need, including both subject matter expertise and funding, and develop a plan of action that will allow the CKB to fully realize its potential of becoming the foundation on which we build the profession. You can be a part of this. As with so many of our other efforts, our members are the key to the success of the CKB, and I urge each of you to consider becoming actively involved in one or more of its component pieces (more information is available on the SARMA web site at [www.sarmapedia.org](http://www.sarmapedia.org)).

**+ Further developing our reputation as a trusted, non-partisan source of information and expertise.** One of the principal reasons behind the foundation of SARMA was the need to fill a void for independent and dispassionate study of the use of risk as a tool for allocating public funding for homeland security activities following the terrorist attacks of 9/11. Some of our greatest contributions to date have come in this area, and I believe this must continue to be a priority. In that regard, two areas where I think it is important for us to focus our energies in the coming year are: 1) assisting the next Administration in developing sound policy on security analysis and risk management issues, and 2) seeking new ways to enhance our relationships within the Department of Homeland Security (DHS) and other federal departments and agencies. I will make the necessary outreach a priority as President, and look forward to providing updates on our progress in future newsletters.

**+ Further developing and strengthening our relationships with other associations and with academia.** One of the most exciting developments of the past year was the emergence of our relationship with the Risk Management Institution of Australasia. Through this burgeoning partnership, SARMA members now have access to a wide array of RMIA projects, conferences, meetings and publications. Equally important is the expanded view and balance these types of contacts bring to our own projects and initiatives. In that regard, efforts are also now underway to explore opportunities to collaborate with several universities in the Washington DC area. Led by our Immediate Past President, Ed Jopeak, these efforts offer great potential, and I look forward to working with him to expand SARMA's contacts and provide additional opportunities to work with other organizations, both in the US and abroad.

**+ Refining the roles and responsibilities of SARMA's Board of Directors and officers.** As SARMA continues to develop and mature as an organization, its leadership must also adapt. Part of this involves elevating the status of the

Board so that it can focus on higher-level issues. Currently, SARMA's Board of Directors and officers meet as a single body. This prevents the Board from focusing on strategic issues and similarly limits SARMA's officers in their ability to drive day-to-day business. At our most recent meeting, the Board took an initial step towards separating these functions by establishing separate meeting schedules for the Board and officers. Other changes are planned, including a continuing effort to recruit established individuals from the public sector, academia and industry to serve on the Board. As Chair of the Nominating Committee, I will continue to work with my Committee colleagues in furthering this important goal.

Finally, as many of you know, DHS has been engaged in an internal review and update of the National Infrastructure Protection Plan (NIPP) for much of the past year. This updated document will soon be released for public comment. Since this is a key piece of national guidance on the use of risk analysis and management in the homeland security enterprise, SARMA intends to provide official comments. However, this should in no way limit any input you may wish to provide individually to DHS. Additional information on how to participate in the public comment period is contained in an article below on the draft NIPP.

In closing, let me say that I hope to hear from many of you in the coming weeks and months about your ideas for how we can continue to build and enhance SARMA. I would also ask you to consider ways in which you can directly contribute, either through the donation of time or other resources. This is, after all, *your* SARMA!

All the best,

Kerry L. Thomas  
President

### Message from Ed Jopeck, Immediate Past President

Now that my two-year term of office as the Founding President of SARMA has come to a close, I am pleased to pass the Presidency torch to Kerry Thomas, a highly dedicated professional and former DHS official who has played a central role in the success of SARMA over the last 16 months. Kerry was elected to the SARMA board in May 2007, and has served the profession and SARMA with distinction as our Executive Vice President. I owe Kerry a tremendous debt of gratitude for his support to and work with me as President, and I have great confidence in his plans and ability to take SARMA boldly into the future.



*Ed Jopeck*

Over the last two years leading SARMA I have had the privilege to work with many intelligent and dedicated security professionals. Among those for whom I am most appreciative are the dozen or so visionaries who first joined me in creating SARMA (when most didn't yet see the need). In addition there are the many selfless volunteers, excellent conference speakers, generous corporate sponsors and other supporters who joined us to make our early success possible. I believe together we have started something important and of lasting historical value: the birth of a new profession that is needed to better secure our nation at a price we can afford. What we are institutionalizing is nothing

less than a revolution in the ways security risks are managed and funding decisions are made.

Fortunately, I will not be going far from the budding success that is SARMA. The Board of Directors has seen fit to create the position of Immediate Past President as a means of providing continuity and transition support to Kerry and future incoming SARMA Presidents. In filling this role I will be supporting the current President by providing assistance with strategic planning, research and special projects. It is a role I relish performing, and I look forward to being even more involved with SARMA's membership, projects and developmental initiatives in the coming months. As always, I invite you to join me; there is much valuable and important work to be done.

In closing, I would like to thank the SARMA Board of Directors, Officers, membership and corporate sponsors for their support these last two years. When we started this journey together there was no recognized security analysis and risk management profession *per se*, and even less recognition of the need for one. Now, only two years later, our efforts are recognized as essential to the success of a variety of national strategies and plans in homeland security, antiterrorism and intelligence. With SARMA's new leadership team and your continued support I am confident that SARMA will continue to develop the profession's knowledge and skills needed by federal agencies, state and local governments and the private sector. It is a daunting task, but having seen the profession respond to this need already, I know that together we are up to the task.

Sincerely,

Edward J. Jopeck  
Immediate Past President

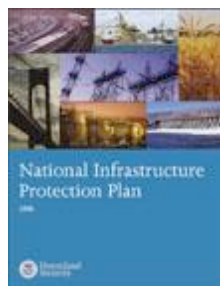
[Return to the top](#)

## News

### DHS Gears Up for Final NIPP Review; SARMA Members Encouraged to Submit Comments

By Avi Klein

As the Department of Homeland Security prepares for its second and final round of public comment on the 2009 National Infrastructure Protection Plan (NIPP), SARMA members are being urged to express their views during what may turn out to be a relatively brief comment period.



The NIPP is viewed as an important document for both DHS and the larger homeland security community. The review and public comment period will provide DHS the opportunity to refine its ideas and plans with regard to risk management and the protection of the nation's critical infrastructures. It also will allow important stakeholders, such as security risk management

professionals, a vehicle through which to offer their expertise in support of homeland security.

Sources familiar with the current draft version of the triennial report -- which is required under Homeland Security Presidential Directive 7 (HSPD-7): Critical Infrastructure Identification, Prioritization, and Protection -- say risk management is treated as the "cornerstone of the NIPP", as it was in earlier versions. In fact, an entire chapter is said to be devoted to articulating both the current state of and a future vision for the NIPP risk management framework. Yet despite this increased emphasis on risk management, said one source, the draft document still does not help its readers understand how to assess risks at multiple levels across all critical infrastructure and key resources (CI/KR) sectors.

Moreover, said one source, despite a clear and growing commitment to security risk management, DHS's own efforts to synchronize such programs internally remain embryonic thus far. This makes it all the more important that the agency take full advantage of the expertise of the broader security risk management profession.

DHS has so far limited its public outreach on the draft to publication in the Federal Register, as required by law.

Larry May of the NIPP Program Management Office told *The Risk Communicator* in late September that his office planned to release the second and final draft for public comment as early as the end of the month, adding that DHS hopes to circulate an amended draft to senior staffers by the end of the year. The previous round of public comments, May said, resulted in only a few responses.

SARMA is now preparing, and plans to submit, formal comments on the latest version. In addition, SARMA members and the professional community at large are encouraged to read and comment on the draft as soon as it is released. It will be published on the NIPP website [www.dhs.gov/nipp ].

*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.*

[Return to the top](#)

## ***Commentary***

### **The Value of Security Risk Analysis: Insights, not Numbers**

*By William L. McGill*

Risk analysis, much like any other professional analytic activity, informs decision-making. Most security professionals have no objections to this seemingly obvious statement. But how does risk analysis actually "inform" decision-making? Do the end results of a risk analysis matter, or is the *process* of doing risk analysis more important?

Much debate in recent years centered on the appropriate arithmetic or logical expression for security risk. It is hard nowadays to call yourself a security risk professional unless you have been party to a debate over the appropriateness of qualitative versus quantitative risk methods -- or perhaps even so-called "quantified" approaches. This debate continues today in government and industry, and is unlikely to subside until the debaters discover the "holy grail" of risk formulas that applies equally well to anything and everything; that is, unless we finally learn to accept that such a formula does not exist, nor would we be much better off even if it did.

A useful risk analysis methodology is one that generates meaningful risk knowledge throughout its implementation. Regardless of the strategy used to score and aggregate threat, vulnerability and consequence, good risk analysis seeks to generate useful knowledge of a system and its weaknesses, and estimates how the system might respond to challenges brought on by a variety of plausible threats. Numbers or labels used to describe risk rarely yield any new insights in themselves. At best, risk results offer a sanity check on methodology and intuition -- and any disagreement between the intuition and the final result provides a means for revealing flawed reasoning or a flawed analytic approach, and nothing more.

I believe that the debate over formula has less to do with the pursuit of mathematical correctness and more to do with it being much easier to argue over equations than it is to debate the "value-add" of a process. Formulas produce visible numbers (whether correct or not); processes generate invisible insights. Consequently, it is harder to measure the benefit of a methodology in terms of its ability to create understanding than it is to criticize the mathematical correctness of an arithmetic expression. But much like the opening statement of this essay, most security professionals would agree that the process of doing analysis is more meaningful than the final answer.

The real question, then, is how do we craft a risk analytic process that maximizes knowledge creation? Shifting the debate toward process instead of product offers the potential for a greater return on intellectual investment than quibbling over details of calculation. After all, it is the reasoning that establishes decision-maker trust in the results of a risk analysis, not the form of the risk output. So let's focus less on how to calculate risk, and more on understanding how to build a methodology that actually improves our ability to make reasoned risk management decisions.

*William L. McGill is an assistant professor of security risk analysis at The Pennsylvania State University. He can be reached at [wmcgill@ist.psu.edu](mailto:wmcgill@ist.psu.edu).*

[Return to the top](#)

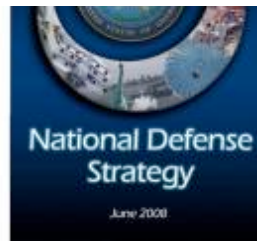
## ***Key Reports and Reviews***

### **National Defense Strategy 2008**

In June 2008 Secretary of Defense Robert Gates issued the National Defense Strategy for 2008. [[Get the](#)



[Report](#)]



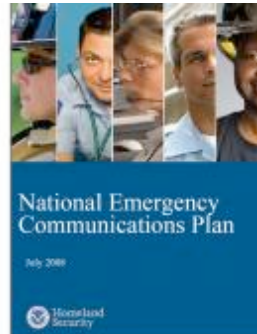
## One Team, One Mission, Securing Our Homeland

In September of 2008 the U.S. Department of Homeland Security released its Strategic Plan for Fiscal Years 2008-2013. [[Get the Report](#)]



## National Emergency Communications Plan

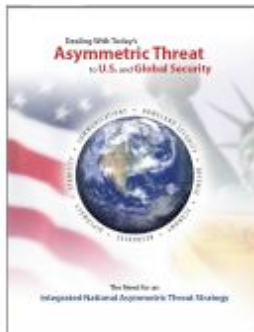
In July 2008 the US Department of Homeland Security released its National Emergency Communications Plan. [[Get the Report](#)]



## Dealing With Today's Asymmetric Threat to U.S. and Global Security

CACI International has published an assessment of the asymmetric threat to US security interests at home and abroad. It is based on ideas presented in a May 2008 symposium, 'Dealing with Today's Asymmetric Threat to U.S. and Global Security,' co-sponsored by the National Defense University (NDU) and CACI International Inc (CACI).

[[Get the Report](#)]



## Towards National Resilience: Good Practices of National Platforms for Disaster Risk Reduction

Prepared by the United Nations  
International Strategy for Disaster  
Reduction (UN/ISDR).

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



## Why Have We Not Been Attacked Again?: Competing and Complementary Hypotheses For Homeland Attack Frequency

"This report examines a number of competing and complementary hypotheses that seek to explain the non-occurrence of a large-scale terrorist attack on the U.S. homeland since 9/11. While the study's title seems implicitly to ask why al-Qaeda has not succeeded in a second homeland attack, the analysis also considers groups within the broader radical Islamist movement as well as non-religious groups and lone individuals."



Prepared by the Science Applications International Corporation (SAIC) and the Defense Threat Reduction Agency (DTRA). [\[Get the Report\]](#)

[Return to the top](#)

## Students' Corner

### SRA Club Targets Wardrivers, Vulnerable Networks



In a world of script kiddies and hackers, it is essential to enable advanced encryption on all private wireless networks. In many cases, small-scale networks common to both homes and small businesses resort to using standard WEP encryption technology (if they use encryption at all), trusting that it provides them with adequate protection against unwanted intrusion. While WEP encryption offers some level of protection, in recent years WEP has become increasingly easy to crack; in fact, the FBI has reported cracking WEP in 3 minutes. The quick and easy solution to this security problem is to enable WPA encryption (packaged with all modern routers). Unfortunately, most homes and businesses are unaware of the advantages of WPA technology over WEP, let alone whether they should even use encryption in the first place.

As a public service to their college and surrounding communities, the Security and Risk Analysis (SRA) Club at the Pennsylvania State University recently began a community "wardriving" campaign in the State College area -- an approximately 4.5-square-mile region in Central Pennsylvania. (Wardriving is the act of searching for Wi-Fi networks by a person in a moving vehicle using

a portable computer or PDA.)

The results of this activity were surprising. Over the course of this two-day exercise, SRA Club members detected 3,356 uniquely identifiable networks. Of these, a staggering 1,214 (36% of the total) were completely unsecure.

Based on this analysis, the SRA club took the initiative to sponsor a community awareness seminar on wireless network security. As part of this program, the SRA Club plans to invite local businesses, homeowners and renters, fraternity representatives, and other networked entities to attend this free event. The seminar will review the differences between WEP and WPA encryption, as well as their pros and cons. It will take the position that it is no longer sufficient to use WEP encryption on one's network, given how easily it can be hacked. Finally, SRA Club members will demonstrate how to successfully apply WPA encryption to a wireless network so as to reduce the chances of losing personal information. The first seminar is scheduled for 29 October 2008, with plans to offer it every month depending on community interest.

Besides these public awareness seminars, plans are underway to map out locations of all unsecure wireless networks using GPS technology and Google Maps. The SRA Club will use a wireless GPS logger to import the coordinates and locations of unprotected wireless routers for the purposes of highlighting intrusion risk hotspots in the State College area. Such knowledge will enable the SRA Club to direct its awareness campaign at specific areas and users in State College so as to minimize intrusion opportunities for determined hackers.

For more information on this and other SRA Club activities, contact the Club's Vice President, Robert M. Tomaro, at [rmt5034@psu.edu](mailto:rmt5034@psu.edu).

[Return to the top](#)

## *Conferences and Training*

### 6th Annual International Counter-Terrorism Officers Association Conference

The International Counter-Terrorism Officers Association is holding its 6th Annual International Counter-Terrorism Officers Conference running from October 21-23, 2008 at the Westin Riverwalk Hotel in San Antonio, TX. [[Go to the Conference Website](#)]

### International Association of Chiefs of Police (IACP) Annual Conference

The International Association of Chiefs of Police will hold its 115th Annual IACP Conference and Exposition in San Diego, California, from November 8-12, 2008. [[Go to the Conference Website](#)]

### 2008 Asia-Pacific Homeland Security Summit & Exposition

The sixth annual Asia-Pacific Homeland Security Summit & Exposition will be held on October 8-10, 2008 in Honolulu, Hawaii.

This year's theme is Scientific Research for Homeland Security: Fostering

International Partnerships.

[\[Go to the Conference Website\]](#)

[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](#)

## *Links of Interest*

[Return to the top](#)