THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION VOLUME 10 NUMBER 12
AND HOMELAND SECURITY

JUNE 2012
CIP/HS UPDATE

EDITORIAL STAFF

EDITORS
Devon Hardy
Olivia Pacheco

STAFF WRITERS
M. Hasan Aijaz

JMU COORDINATORS
Ben Delp
Ken Newbold

PUBLISHER
Liz Hale-Salice

Contact: dhardy1@gmu.edu
703.993.8591

Click here to subscribe. Visit us online for this and other issues at http://cip.gmu.edu

In this month's issue of *The CIP Report*, we highlight some of the activities and projects that the Center for Infrastructure Protection and Homeland Security (CIP/HS) has been developing and working on since the last CIP/HS update in August 2010.

GEORGE MASON UNIVERSITY
School of Law
CENTER for INFRASTRUCTURE PROTECTION and HOMELAND SECURITY

First, we describe our involvement with The Infrastructure Security Partnership's (TISP) *2012 Critical Infrastructure Symposium: Full Spectrum Resilience*. One of our co-hosts for the *2012 Critical Infrastructure Symposium*, along with the Coordinator and Principal Instructor with the Infrastructure Protection and International Security Program at The Norman Paterson School of International Affairs at Carleton University, then illustrate the concept of Full Spectrum Resilience (FSR). We explain our support to the Department of Defense's Uniformed Services University of Health Sciences Center for Disaster and Humanitarian Assistance Medicine (CDHAM). The CEO of Personal Recovery Concepts, LLC and two representatives from First Response Solutions Incorporated illustrate the significance of personal resilience and provide information on the CIP/HS Personal Recovery Concepts program that combines training and testing of individual continuity of operations (COOP) roles and responsibilities with family preparedness. Next, we provide an update on the KEPCO International Nuclear Graduate School (K-INGS) degree program. We also discuss several of the events we have co-hosted with Pepperdine University, The Security Analysis and Risk Management Association (SARMA), InfraGard, and supply chain associations in the last year. Finally, our partner institution, James Madison University, provides an update on their activities and programs.

We hope you enjoy this issue of *The CIP Report* and find it useful and informative. Thank you for your support and feedback. For this issue, we would especially like to thank our collaborative partners.

Mick Kicklighter
Director, CIP/HS
George Mason University, School of Law

The 2012 Critical Infrastructure Symposium

In April 2012, CIP/HS was honored to co-host the *2012 Critical Infrastructure Symposium: Full Spectrum Resilience* with The Infrastructure Security Partnership (TISP), West Point, and the Society of American Military Engineers. The event, which was held from April 23-24 in Arlington, VA, sought to engage and foster discussion with the academic community, including undergraduate and graduate students, as well as industry professionals and government officials who conduct research and/or work in the field of critical infrastructure protection and resilience. While this article will be followed by a summary on the concept of Full Spectrum Resilience, this article focuses on the hosting responsibilities of CIP/HS.

As one of the hosts for the event, CIP/HS was responsible for presenting during the morning workshop on April 23. The workshop, entitled "Infrastructure Higher Education," provided CIP/HS the opportunity to update representatives from the government and private sectors and the academic community on its education program. CIP/HS was joined by Colonel (Retired) Robert Stephan, Executive Vice President of CRA, and Sarah Miller Beebe, Owner of Ascendant Analytics LLC.

The purpose of the "Infrastructure Higher Education Workshop" was to: 1) provide an overview of the goals and objectives of the education project; 2) gather input/feedback on the practicality and effectiveness of the developed materials to advance the knowledge and skills of professionals who are involved in protecting critical infrastructure; and 3) share an example of a pedagogical best practice case study that can be utilized in coursework.

The workshop was divided into three presentations. CIP/HS provided an overview of the education program while Col. Stephan described the curriculum evaluation process and Ms. Beebe demonstrated the usefulness of case studies. During the first presentation, CIP/HS explained that the mission of the education program, which was initiated in 2010 and featured in the August 2010 issue of *The CIP Report*, is to create a comprehensive, unified approach to homeland security education. The long-term objective of this project is to ensure that a cadre of professionals responsible for protecting the Nation's critical infrastructure is developed and maintained. To complete this goal, CIP/HS developed critical infrastructure protection materials and shared these resources, including syllabi, with other colleges and universities and interested organizations. The first year of the project started with an assessment of existing courses, concentrations/minors, degree programs, and training programs in critical infrastructure protection; instruction on the seven critical infrastructure protection competency areas;[1] and use of best practices. This assessment resulted in the development of seven stand-alone critical infrastructure protection courses/syllabi that are deployable within multiple degrees at schools of business, public policy, engineering, science, health, government, etc. These resources are currently available on the CIP/HS website. The second year of the project, which began in June 2011 and completed in May 2012, created a five-course certificate program in critical infrastructure protection; modified existing courses from a Public Administration program to include a concentration in critical infrastructure protection; compiled a library of critical infrastructure protection reading materials and a roster of subject-matter experts; created a case study for the classroom on the I-35W bridge collapse in 2007 in Minnesota; and evaluated the certificate and graduate curricula.

(Continued on Page 3)

[1] The critical infrastructure competency areas, identified in the 2009 National Infrastructure Protection Plan (NIPP), include: Risk Analysis; Protective Measures/Mitigation Strategies Development; Technical and Tactical Expertise (Sector-Specific); Partnership Building/Networking; Metrics and Program Evaluation; Information Collection and Reporting (Information Sharing); and Program Management. Please see page 84 of the 2009 NIPP for more detailed information.

TISP *(Cont. from 2)*

Col. Stephan, who presented second, described the extensive curriculum evaluation process. As he explained, the purpose of evaluating the certificate and graduate courses was to ensure that the curricula meets the current and future needs of the infrastructure protection profession; establish education standards for future infrastructure protection leaders and the professional workforce; and; provide recommendations for long-term planning. The curriculum evaluation process involved the following tasks: identification of curriculum goals and objectives; creation of a curriculum evaluation guide; selection of subject-matter experts; evaluation of curriculum; and the development of long-term recommendations. The curriculum goals and objectives are listed in each syllabus, but they are based on the seven critical infrastructure protection competency areas. In terms of higher education goals and objectives, the content; pacing; learning activities; assessments; learning resources; and overall course design were also reviewed. The curriculum guide, created by CIP/HS, simplified the review process for the subject-matter experts reviewing the curriculum. Their response to the evaluation guide helped CIP/HS answer such questions as are the courses academically rigorous? Is there enough content? Is there too much content? Is the content missing anything? Do the best practices foster critical thinking and practical application of knowledge? Is there enough content on the sectors and/or specific topics (i.e., international critical infrastructure, leadership and management, report writing, and risk analysis)? Do the courses meet the needs of the job market? What is the job market? How can the courses be maintained and updated? What is the best method(s) of deployment? Following Col. Stephan's presentation, the enthusiastic participants of the workshop provided their own answers to these questions, thereby contributing their valuable experience to the education program to ensure that the courses are academically relevant and rigorous.

Ms. Beebe, who presented last, but certainly provided the most entertainment, provided a demonstration on the I-35W bridge collapse case study that was developed during the second year. As she explained, given that the use of case studies in the classroom fosters critical thinking and practical application of knowledge, it is an effective higher education best practice. As she illustrated, case studies reinforce key concepts and lexicon; bridge theory and practice; model question-driven analysis; engage learners in active, hands-on learning; drive home the principles of critical thinking; reinforce effective collaborative processes; and provide a practical and repeatable analytic framework for future challenges. She explained that the I-35W bridge collapse was selected as the initial case study because it highlights the challenges of planning and response in a high-vulnerability, multi-threat environment that is a nexus of multiple infrastructure modes. This particular case study is separated into two parts: the learner version and the instructor version. The learner version includes key questions; the narrative; recommended reading; and exercises, including structured brainstorming, hypothesis generation, and starbursting, with value added questions. The instructor version includes the instructor introduction; notional exercise solutions; case conclusion; and key takeaways. Once the mechanics of the case study were described, Ms. Beebe then demonstrated the usefulness of the case study by engaging with symposium participants.

The products that were developed for the second year, including the syllabi for the five certificate courses, the list of infrastructure protection reading materials, and the case study, will soon be available on the CIP/HS website. CIP/HS sincerely encourages the use of these materials; in fact, the effectiveness of the education program is fundamentally dependent upon feedback from the government and private sectors as well as the academic community. This will ensure that input from experts and leaders in the field of critical infrastructure protection is incorporated into the curriculum, thus improving upon the foundation that has already been developed.

All of the symposium presentations, including the workshop presentations, are currently available

(Continued on Page 24)

Full Spectrum Resilience: An Executive Summary

by E. Wayne Boone, Ph.D., PCIP
Coordinator and Principal Instructor, Infrastructure Protection and International Security Program at The Norman Paterson School of International Affairs, Carleton University;
and Steven D. Hart, Ph.D., P.E.
Engineer Research and Development Center (ERDC) Engineering Fellow at West Point

The concept of Full Spectrum Resilience was both the theme and topic of the opening presentation at the *2012 Critical Infrastructure Symposium*. While the full paper on this topic will be published in the Symposium Proceedings in the Homeland Security Review, this article provides a brief summary.

Over the past 50 years, the rise of our interconnected, interdependent society combined with terrorist attacks and natural disasters has resulted in the development of both scholarly, practical, and government works in critical infrastructure protection and resilience. This growth can be demonstrated in a search of the Homeland Security Digital Library, which will return over 35,674 items on "critical infrastructure," 32,812 on "critical infrastructure protection," and 6,895 on "critical infrastructure resilience." With this profusion of publications, how does one establish the relationship of one document to another and all documents to the body of knowledge as a whole?

The concept of ***Full Spectrum Resilience*** (FSR) provides an effective organizing principle which relates individual elements of critical infrastructure work and scholarship to each other and to the body as a whole. It can also assist in the formation of a coherent infrastructure resilience doctrine. The elements of doctrine, resilience, and full spectrum will be treated in turn.

Doctrine

At its root, doctrine is simply an agreed upon set of principles and concepts that organize, unite, and guide organizational activities. Doctrine can be taught to new members of the organization, used as a basis for training plans, serve as a standard for evaluation of drills and exercises, and validate decisions taken. One approach to establishing doctrine is top-down authoritative direction; in the case of critical infrastructure, this approach would probably result in large volumes of paper suitable only for starting fires or house-breaking a new puppy. An alternative, supported by the concept of FSR, is establishment of doctrine from within the professional community in a collaborative manner to reach consensus on existing and emergent critical infrastructure protection and resilience (CIP/R) principles and concepts. FSR provides the framework; the expertise of practitioners at all levels and stages of operations, combined with scholarly research of academia and informed by the input of business owners and managers, provide the best practices, validated principles, and fundamental concepts.

Resilience

The terrorist attacks of 2001 gave us a desire for infrastructure protection. The hurricane season of 2005 gave us the desire for infrastructure resilience. While many definitions have been offered for resilience, The Infrastructure Security Partnership's definition of resilience as "a capacity to absorb or mitigate the impact of hazard events while maintaining and restoring critical services"[1] seems to work best as the basis for FSR doctrine. The requirement for resilience is based on the premise that protective, preventive, and deterrent safeguards will not always be effective (i.e., successful in keeping out a threat) and therefore will require response, recovery, and restorative action.

(Continued on Page 5)

[1.] The Infrastructure Security Partnership, White Paper for the White House Office of Critical Infrastructure Protection and Resilience Policy and Strategy, Alexandria, VA: The Infratructure Security Partnership, (2010).

Resilience *(Cont. from 4)*

Therefore, by definition, prevention, response, and recovery are all elements of resilience.

Full Spectrum

The concept of FSR draws on principles learned from military doctrine to establish a coherent framework for thinking about all related aspects of resilience and the body of knowledge as a whole. Based on three aspects, it is proposed as a relational concept to integrate understanding and organize, rather than limit, creative thought.

Drawing on the levels of war, the first aspect is the *Levels of Resilience:* strategic, operational, and tactical. Strategic Resilience includes the establishment of policies and objectives to achieve broad, long range goals; the allocation of resources; the integration of all elements of the organization to support those goals; and a statement of the acceptable risk that senior management is willing to assume in the operation of a critical infrastructure (CI). Strategic Resilience takes place over a long period of time and does not respond to slight, or even some moderate, variations in situations. Operational Resilience involves the interaction of specific actions, programs, and initiatives to achieve more focused objectives over broad reaches of space, time, and participants. The successful completion of several operational objectives leads to the successful attainment of strategic objectives. Tactical Resilience refers to specific actions taken in specific circumstances designed to achieve a specific short-term end. Given their concrete nature, tactical resilience initiatives tend to be easier to measure in terms of success when compared to higher level resilience objectives. For an organizational entity to be resilient, all Levels of Resilience must be addressed across a range of potential impacts.

The second aspect of FSR requires consideration of the *Range of Impact* of a threat or hazard successfully exploiting a vulnerability to affect the operation of a CI. A National level impact touches multiple states, regions, organizations, professions, and groups. It covers topics that are of common or related interest across this space. The level below National is Regional, as opposed to State, province, or territory since neither CIs nor impacts typically respect political boundaries. Furthermore, entities on either side of these political boundaries are more often united by common interests than divided by a line on a map. Regions are subdivided into Communities, which are smaller in scale yet still united by common factors such as political organization, watershed, levee district, or business interests. Communities may form and dissolve around specific concerns or interests that arise and then are satisfied. An entity, say a town, business, or organization, may be a member of several communities and thus have several different, and perhaps competing, interests. Most emergencies take place at the local level and are managed by the community or municipalities affected.[2] The final level is Individual, which includes persons and their immediate families living in the same household. While the interests and actions of individuals are part of communities and regions, individuals also act out of their own self-interest and are, by definition, the first to respond to their own personal emergencies.

The third aspect is the *All Hazards Environment.* FSR requires the consideration of deliberate malicious acts (e.g., terrorism, disgruntled employee, or vandalism), earth effects and natural disasters, accidents, and deterioration. While the results of many elements in the All-Hazards Environment may be similar with a resulting similarity in response and recovery, the causes and therefore the actions taken in prevention or mitigation are very different. For example, a terrorist bombing of a propane tank and a car leaving the road and striking the propane tank cause the same explosion, but must be prevented in different ways while the aftermath is treated in a similar way. Failing to consider all elements of the All-Hazards Environment will result in partial, not full-spectrum, resilience.

FSR as an Organizing Concept

The Levels of Resilience (strategic, operational, tactical), Range of Impacts (national, regional, community, and individual), and the All-Hazards Environment (earth effects, deliberate malicious acts, accidents, and deterioration) can

(Continued on Page 6)

2. Public Safety Canada, *An Emergency Management Framework for Canada,* Government of Canada, (2011).

Resilience *(Cont. from 5)*

combine in a cubic arrangement to form the concept of FSR shown in Figure 1. Yes, it is the "Rubik's Cube[3]" of resilience.

This matrix and its 48 "bins" allow for the classification and analytical isolation of any work. For example, the National Infrastructure Protection Plan (NIPP) is a strategic level document that addresses the four elements of the All-Hazards Environment at the National level. The model earthquake design codes[4] produced by the National Earthquake Hazard Reduction Program (NEHRP) are tactical level documents that deal only with earthquakes at a Community level. Even though they are produced at a National level, the NEHRP model codes are implemented at the tactical level of resilience. They are focused on specific actions taken in specific circumstances to achieve a specific end.

The concept of FSR can aid in integrating resilience thinking in three principal ways. First, it allows us to make positive statements of what something is, as demonstrated above, which then indicates what it is not. This keeps us from expecting a result that a program cannot deliver. When the NIPP is classified in the FSR concept as strategic-all-hazards-national, we cannot expect it to improve the resilience of the 22nd Street Bridge. Second, it allows us to relate one program to another. For example, TISP's Regional Disaster Resilience Guide (RDRG)[5] complements the NIPP because it is an operational level document focused at the Regional and Community levels dealing with disasters and terrorism. Third, it allows us to identify the gaps in our comprehensive approach to resilience. If the NIPP satisfies the strategic-national-disaster bin and the RDRG satisfies the operational-regional and community-disaster bins, what satisfies the tactical-regional, community, and individual-disaster bins? Without tactical programs to address specific needs at specific locations in specific circumstances, we cannot achieve FSR.

Figure 1: Full Spectrum Resilience.

Conclusion

Full Spectrum Resilience is a doctrinal concept to formulate all of the scholarship, research, publications, codes, and standards for protection into a coherent whole. It does not require anyone or anything new except a positive statement at the beginning of a work which might say "this is a tactical level work focused on deterioration at the individual bridge." If this concept is adopted by our community of practice, then our doctrine — a commonly

(Continued on Page 24)

3. This game was developed in 1974 by Hungarian Emo Rubik, a professor of Architecture at the Academy of Applied Arts and Crafts in Budapest. Its actual purpose was to assist in solving the structural problem of moving parts independently without the entire mechanism falling apart. It only became a puzzle when Rubik scrambled the tool and then tried to restore it. http://en.wikipedia.org/wiki/Rubik's_Cube, accessed April 3, 2012.

4. The NEHRP guidelines and codes are available at www.nehrp.gov/resources/guidance.htm or through the Federal Emergency Management Agency site at http://www.fema.gov/plan/prevent/earthquake/codes.shtm (Federal Emergency Management Agency National Earthquake Hazards Reduction Program).

5. The Infrastructure Security Partnership's Regional Disaster Resilience: A Guide For Developing An Action Plan 2011 Edition is available from the TISP site at www.tisp.org/.

The Cooperative Biological Engagement Program: Twenty Years and Counting

On December 12, 1991, President George H.W. Bush signed into law the Nunn-Lugar Amendment 86-8. Two weeks earlier, Senators Sam Nunn and Richard Lugar had gathered senate colleagues to hear about the imminent collapse of the Soviet Union and the potential threats that may result from the loss of control over Soviet weapons of mass destruction (WMD). Two weeks after the President had signed the bill, the Soviet Union collapsed and the threat became a reality. Twenty years later, the Cooperative Threat Reduction (CTR) Program that Nunn-Lugar initiated is continuing the pioneering work of those far-sighted Senators. The achievements of the program are documented in the Nunn-Lugar Scorecards, which are accessible at http://www.dtra.mil/Missions/NunLugar/scorecards.aspx. The CTR program, based at the Defense Threat Reduction Agency (DTRA), still encompasses nuclear, chemical, and biological threats. But, in recent years it has expanded beyond the initial focus of the Soviet Union to embrace a broader set of new partnerships around the world. In accordance with U.S. national security concerns, the program has increasingly focused on the biological threat. The objectives of the DTRA Cooperative Biological Engagement Program (CBEP) are to cooperatively assist partner nation governments in addressing obligations assumed by signing the United Nations (UN) National Security Council Resolution 1540 as well as the World Health Organization's (WHO) International Health Regulations (IHR). Resolution 1540 seeks to prevent the proliferation of nuclear, chemical, and biological weapons, as well as their means of delivery, which includes the establishment of controls over related materials, while the WHO IHR aim to enhance national, regional, and global public health security.

CBEP, focusing on the biological agents, employs a multi-pronged approach to meet its objectives by providing education and training to enhance clinical, laboratory, and epidemiological safety and security with regard to especially dangerous pathogens (EDPs). CBEP also works to strengthen the partner nation's detection, diagnostic, and reporting systems, as well as fund and conduct academic and scientific research on EDPs. CBEP adheres to the United States Government's (USG) whole of government approach to engage with partner nations. For example, CBEP works in coordination with the U.S. State Department, United States Agency for International Development (USAID), the Centers for Disease Control and Prevention (CDC), and the United States Combatant Commands to ensure that the program is structured to provide maximum support to the partner nation. George Mason University (Mason), through CIP/HS, provides support to the Department of Defense's Uniformed Services University of Health Sciences Center for Disaster and Humanitarian Assistance Medicine (CDHAM). The CIP/HS work with CDHAM is providing technical expertise that is helping to support the CBEP and to develop processes and tools that facilitate the expanding work of CBEP with partner countries. The initial outputs from the CIP/HS-CDHAM team include a Requirements Validation Process (RVP) that can help to identify the policy, legal frameworks, and the capacities and capabilities of partner country systems for the detection, diagnosis, and reporting of diseases that are caused by EDPs. Once complete, the RVP provides a baseline enabling both CBEP and the partner country to identify a mutually agreed upon path forward to strengthen and augment the partner nation's ability to meet its obligations under UN 1540 and the WHO IHRs.

In celebrating 20 years of Nunn-Lugar, the Nuclear Threat Initiative (Washington D.C.) noted "Nunn-Lugar is not merely a program or a funding source or a set of agreements. It is an engine of expertise and cooperation that can be applied around the world — and must be. To meet the threats of the 21st century, the United States must send the clear message that we are willing to go anywhere to reduce the threats of WMD — the most

(Continued on Page 24)

Eliminating the Critical Gap in Emergency Response Plans

by Ann Coss, Personal Recovery Concepts, LLC, and
Charles W. Newsome and Jim Wong, First Response Solutions, Inc.

In the post-September 11 era, a majority of medium-to-large organizations in both the public and private sectors — at the urging of the government and out of self-interest — have developed and deployed emergency response plans. Many of these organizations have extended this proactive preparedness to include planning for the unique requirements of disaster recovery and business continuity.

Yet, despite the expenditure of billions of dollars and the efforts of emergency planners, it has become painfully evident in the aftermath of catastrophes like Hurricane Katrina on the Gulf Coast, where 770,000 people were displaced, and the more recent Joplin, Missouri tornadoes that even the most anticipatory and robust emergency plans can suffer from a fatal omission: the critical role played by individual employees, whether uniformed first responders, utility workers, healthcare workers, or workers in other sectors of the economy that deliver critical manufacturing or support services.

Most Organizational Resilience plans currently in place start the clock running in the aftermath of a disaster with the incorrect assumption that employees can typically be relied upon to report to work promptly and implement emergency response procedures. But, what if this assumption is fundamentally wrong? What if phones and desks remain unmanned, response vehicles remain silent in their garages, and other critical responsibilities remain unmet because there are not enough employees on hand to fulfill the organization's mission when a major disruption occurs? Tragically, this scenario has played itself out numerous times throughout the country in recent years.

But this conundrum is not inevitable, and can be ameliorated over time through the deployment of robust and user friendly new technologies and methodologies that address the "fatal omission" of personal resilience. This article endeavors to explain how Organizational Resilience is strategically linked to the personal preparedness of any organization's employees. It will demonstrate how increased employee availability has become the linchpin to rapid recovery and organizational survival, especially in today's climate of asynchronous threat. It will also provide information on a certificate program deployed at Mason that seeks to address personal resilience.

Nature is part of the threat we face every year. According to the Federal Emergency Management Agency (FEMA), there were 99 major disaster declarations around the country in 2011, with 12 that exceeded a billion dollars in costs. These figures represent the tip of the iceberg. For example, the 2011 adjusted estimate of damage from Hurricane Katrina alone is $145 billion. How much of this cost could have been avoided is theoretical. However, in these tough economic times, it is axiomatic that most organizations, both in the public and private sectors, are working under severe budget and fiscal constraints. Therefore, this article will also demonstrate a robust business continuity planning model that will help organizations maximize their return on investment and the synergy between personal preparedness and continuity of operations.

Since September 11, when both the government and private sectors began to keep rigorous statistics on disaster management, rapid recovery has become a leading indicator of organizational survival and post-incident viability. For example, statistics from the last ten years show that:

- 25 percent of businesses do not reopen following a major disaster;
- 75 percent of organizations without a business continuity plan fail within three years;
- Companies not up and running

(Continued on Page 9)

PRC *(Cont. from 8)*

within 10 days face low odds of surviving;
- 43 percent of those without a continuity plan never reopen; and
- Of those that reopen, only 29 percent are still around two years later.

The National Infrastructure Advisory Council (NIAC) was formed shortly after September 11. The NIAC is comprised of 30 bipartisan members from both the public and private sectors. The council's job is to advise the President on how to safeguard the Nation's critical infrastructure, currently divided into 18 sectors. In September 2009, the NIAC published a rigorous definition of infrastructure resilience, and recommended to the President that public-private sector collaboration is the only way to protect this country's critical infrastructure.

Among the many contributions the NIAC has made, perhaps the most useful has been the definition of resilience, commonly referred to as "the 3Rs:"

Robustness: The ability to maintain critical operations and functions in the face of crisis.

Resourcefulness: The ability to skillfully prepare for, respond to, and manage a crisis or disruption as it unfolds

Rapid Recovery: The ability to return to and/or reconstitute normal operations as quickly and efficiently as possible after a disruption.

As can be seen, "people" are the ultimate foundation to the 3Rs. It is also easy to see why Rapid Recovery has become a leading predictor, and plays such a critical role, in Organizational Resilience. In this regard, it can be asserted that people are America's 19th critical infrastructure, undergirding the U.S. economy and safeguarding our way of life.

So, let us look at the current typical

(Continued on Page 10)

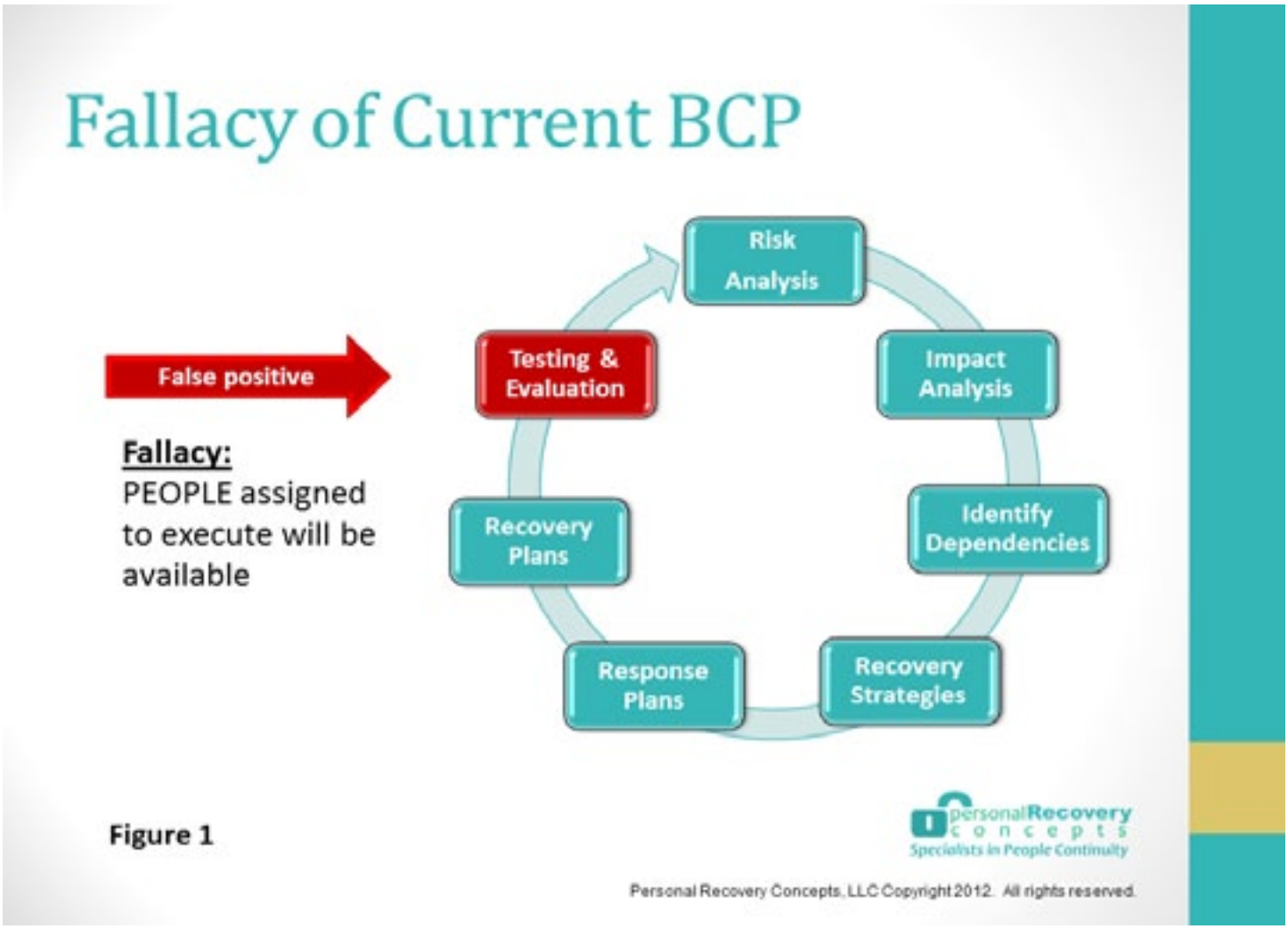

Figure 1

PRC *(Cont. from 9)*

planning model for business continuity protection (See Figure 1 on Page 9). Most emergency planners have gone through each step from Risk Analysis to Testing and Evaluation. Whether organizations conduct this last step as a tabletop exercise or actual drill, testing is typically done under conditions where, psychologically, the employee knows his family is safe and secure and he is not worried about his own ability to recover and rebuild. Under these conditions, testing frequently produces a false positive about Organizational Resilience, as measured by the 3Rs. The fallacy is in assuming that people assigned to execute will be available.

Uniformed first responders constitute a meager one percent of the U.S. population. But, statistics after Katrina, Joplin, and other disasters show that this tiny fraction of our population, entrusted with carrying the day for the rest of the 99 percent of us in the event of a disaster, first check on their own families in the immediate aftermath of the event. Who can blame them? The survival instinct is innate in each of us, and the impulse to first protect one's own is the product of a million years of evolution and thousands of years of human ethics and religious tradition. At the end of the day, we are defined more by our private lives — our families and our homes — than we are by our employment, however noble and proud the traditions of our jobs might be.

According to the American Red Cross, only seven percent of Americans have any plan for their own personal recovery, effectively delaying the time it takes them to be available to the organizations that rely on them, especially when they are victims of a disaster. When a delay in the time it takes a key employee to respond occurs, or when the focus he can apply to his duties is diminished, mission success is jeopardized.

It is important to note that so much sophisticated technology is deployed nowadays that we tend to forget that this technology is wholly dependent upon the cadre of employees trained to use it. Without these key individuals at their stations, even the best laid plans simply cannot be executed. Organizational Resilience inevitably depends upon the personal preparedness of individuals, and their availability to "execute," both during and after an event.

Presidential Policy Directive 8: National Preparedness (PPD-8), issued in March 2011, established a national mandate to create a plan for shared responsibility amongst all levels of government, the private sector, and individual citizens to safeguard the Nation from harm. PPD-8 follows a spate of Federal directives designed to help standardize continuity management across agencies, including: National Security Presidential Directive-51/ Homeland Security Presidential Directive-20, National Continuity Policy Implementation Plan of 2007, and Federal Continuity Directives 1 and 2 (FCD 1/2) of 2008.

FCD 1 was developed to guide governmental continuity planning efforts and to share best practices based on lessons learned with private sector stakeholders. This planning requirement includes a provision for individual preparedness, as follows: "…provide support and guidance to all staff in developing family support plans which will increase personal and family preparedness throughout the organization and support employee availability during a continuity event."[1]

Significantly, the ASIS Organizational Resilience Standard states: "[i]t is no longer enough to draft a response plan that anticipates disasters or emergency scenarios. Today's threats require the creation of an on-going, dynamic, and interactive process that serves to assure the continuation of an organization's core activities, before, during. and — most importantly — after a major crisis."[2]

In an All-Community environment, the lack of individual preparedness, whether in the case of a first responder or a corporate employee, can profoundly jeopardize the 3Rs, or the ability of a community to recover overall. The ultimate goal of the employer is to implement a plan that optimizes the employee's

(Continued on Page 11)

1. http://www.fema.gov/pdf/about/offices/fcd1.pdf.
2. http://www.asisonline.org/guidelines/or.xml.

PRC *(Cont. from 10)*

ability/desire to report to work under adverse circumstances. The employee ultimately has the same goal: return to work and make money. But that is both the opportunity and the rub — what an employee needs to do to recover in their individual life and what they need to do to get to the point where they feel able to report to work is exactly the same.

Before he feels capable of responding to work, an individual needs to accomplish a set of key personal requirements, like providing for basic needs, arranging temporary shelter, and making an insurance claim. This is why the standards have evolved to include planning after a major crisis. In other words, how long it takes an employee to conduct these personal recovery activities is what impacts his organization's workforce productivity and related costs.

An improved model for creating Organizational Resilience will incorporate two additional steps: 1) risk analysis, to include the impact of family preparedness on the individual's ability to execute; and 2) individual preparedness of critical team members. In other words, a "People Continuity Plan," akin to a "Business Continuity Plan," specific to an individual's role and responsibility both at home and at work.

There are five key areas of personal resilience or preparedness that will improve employee recovery time: Personal, Financial, Emergency, Household, and Legal. Once these categories are fully acknowledged, accommodated, and planned for, an integrated plan is in place which both fundamentally empowers the individual and dovetails synergistically with the employer's existing overall emergency response planning. Risk Management is a task that focuses on limiting exposure. By contrast, Organizational Resilience is a competitive strategy that addresses critical gaps in the risk management model and incorporates the 3 R's. Simply stated, Risk Management is a task to minimize exposure, whereas Organizational Resilience is a competitive strategy, capitalizing on people as the fundamental building block of resilience, helping organizations act proactively to improve their Robustness, Resourcefulness, and Rapid Recovery. Bottom line: Organizational Resilience is a smart investment with a high return.

Undeniably, people are the linchpin; yet according to Forrester, 75 percent of all emergency plans in place do not support personal resilience.[3] Also, according to FEMA's Preparedness in America Survey, released in June 2009, we know that only one percent of the population has a complete second set of identification and that only two percent have documented their financial accounts or assets. Couple this report with the American Red Cross statistic that only seven percent of Americans have taken any basic preparedness steps (meaning that some 93 percent of our workforce is not ready or resilient, that 93 percent of our community is not ready or resilient, and that 93 percent of our supply chain is not ready or resilient), factor in that 39 percent of small businesses have no continuity plan at all, and we are left with one disruptive event that economically impacts an entire community. In a word, we are left with an economic domino effect where if an individual cannot recover, the community cannot recover, and businesses do not have customers. So, revenue quits flowing, which means no tax revenue at the local, State, or Federal levels. Therefore, we need a paradigm shift which enables organizations to transform interdependence from a liability to a net asset, before, during, and following a disaster.

Elements of a Comprehensive Personal Resilience Program

The first task is to incorporate individual preparedness within the standard emergency planning process within the organization. An effective program should follow a standards-compliant "plan, do, check, act" model.

As integrating personal resilience with organizational emergency planning invariably requires individuals to learn and adopt new habits, the learning management system should encompass efficient company-wide training, capitalizing on capabilities like interactive workshops, supported by robust data collection software to identify, collect, and collate all of

(Continued on Page 12)

[3] Forrester Research, *Work Force Continuity: A Critical Strategy in Your Business Continuity,* (December 2006), www.forester.com/home.

PRC *(Cont. from 11)*

the personal data gathered.

The standard training should be designed to help an individual actually create a dynamic plan. For instance, the program should not merely indicate that an individual needs to know their Specific Area Message Encoding (SAME) number to program the weather radio. Rather, since disaster recovery is SAME dependent, the client should be instructed that they need to know it, and then be asked to click a link which takes them directly to their geographic SAME number so that it is displayed and can be recorded. This type of hands-on preparatory training is instrumental in reducing chaos during a real crisis.

Equally important, the workshop should be customizable so as to include the organization's plans specific to the employee and their individual role and responsibilities. The logic is simple: whether or not an employee is managing a job that requires years of training or experience, prolonged absences can have unpredictable consequences that are challenging for any organization to manage, even in normal situations. A multi-week course should be offered, guided by an expert in personal resilience. This will allow time for the employee and their family to prepare their own personal resilience plan, under the tutelage of a resilience expert. If the organization prefers, the course should have the flexibility to be taught within a train-the trainer scenario. Designed correctly, all of these options should be part of a turnkey, automated learning management system that helps to ensure that the right people are available to minimize disruptions during and following a continuity event. For anyone who has witnessed or lived through role conflicts during a disaster, this resilience education is designed to minimize if not prevent the chaos.

The system should also incorporate robust reporting capabilities, allowing management to extract pre-programmed reports or to create customized reports for export into commonly utilized formats like HTML, PDF, CSV, Excel, Word, OpenOffice or RTF. With this capability in place, reports can then be automatically generated and e-mailed to a predetermined set of stakeholders, as an integral component of the Plan, Do, Check, Act protocol.

The Bottom Line

Leading global reinsurer Swiss Re reported that, in 2011, total economic losses to society due to disasters (both insured and uninsured) reached an unprecedented $370 billion, compared with $226 billion in 2010. Contributing to the record year in 2011 was the earthquake in Japan, which accounted for 57 percent of the world's losses. With insured losses accounting for only $116 billion last year, the lion's share of the $370 billion was borne by the private sector, to include individuals. It is important to note that economic losses only capture part of the picture. Although losses are measured in dollars, these numbers do not indicate the time it takes to rebuild a community or the human toll of a disaster. Whether it is a natural or a man-made disruptive event, financial losses are inextricably linked to human suffering.

Given that first responders comprise only one percent of the U.S. population, and that their availability is unquestionably critical to stemming human as well as property losses, it is in every community's best interest to guarantee the personal resilience of this small group, including their families. Correspondingly, since approximately 85 percent of America's critical infrastructure is in the hands of the private sector, it also makes good business sense to similarly safeguard the resilience of individuals who occupy key positions in these all-important segments of the U.S. economy. If PPD-8 is designed to protect the American way of life, plans and policies must especially focus on small businesses. According to the Small Business Administration, small businesses make up some 97 percent of employers, contributing to almost half of U.S. payroll, and are historically the most vulnerable to disasters.

In the end, only when Organizational Resilience is strategically and functionally linked to the Personal Preparedness of individual employees within any organization's contingency plan can disaster recovery and business continuity plans be truly effective. When disaster strikes,

(Continued on Page 24)

KEPCO International Nuclear Graduate School (KINGS) Summer Study Program

During the months of June and July 2012, Korean students will attend noncredit classes on the Fairfax Campus of George Mason University as part of the KEPCO International Nuclear Graduate School (K-INGS) degree program. This is anticipated to become an annual occurrence, although the number of students attending will vary in future years.

The 2012 "class" consists of 32 students. They range from 24 to 43 years of age with the median age being 33. They are predominately practicing professionals in the field of nuclear power plant management or related professions. They are enrolled in either a two year program at KINGS, which will result in the award of a master's degree, or a three year program that will result in the award of a doctorate. These degrees will be awarded by KINGS in accordance with the rules and regulations governing such degrees in Korea and are not directly comparable to degrees awarded by accredited colleges in the United States.

The students will attend classes in accordance with a schedule developed by the Volgeneau School's Systems Engineering and Operations Research Department (SEOR). The 2012 class will be taught in a single cohort for approximately six hours per day, Monday through Friday (subject to change). The courses are condensed versions of classes currently taught at Mason with an emphasis on group projects and collaborative learning. Guess speakers, or trips to meet key policy-makers, will be programmed into their time at Mason. The intent is to provide four such opportunities during the approximate eight weeks they are at Mason.

In addition to the course work, the program will provide opportunities for the students to experience local American culture. There will be a welcome dinner and a dinner/graduation ceremony at the end of the course held at the Mason Inn. Mason's Office of Continuing Professional Education (OCPE) will provide appropriate certificates documenting the completion of the course work. CIP/HS is honored to be coordinating these opportunities.

For more information about the origins of the project, please review the August 2010 issue of *The CIP Report* at: http://cip.gmu.edu/archive/CIPHS_TheCIPReport_August2010_CIPHSUpdate.pdf. For more information about this program, please visit: http://www.k-ings.ac.kr/web/www. ❖

Phtoto courtesy of the K-INGS website.

Leadership, Advocacy, and Policy Development Workshop with the Pepperdine University Doctoral Program in Organizational Leadership

CIP/HS welcomed the Pepperdine University Doctoral Program in Organizational Leadership to Mason on May 4, 2012. This day of dialogue and presentations about challenges in leadership marked the second event of its kind in the CIP/HS-Pepperdine partnership and yielded valuable insights into the leadership aspects of infrastructure protection.

The day opened with presentations from CIP/HS Director LTG (ret) Mick Kicklighter and Board Member Dr. William Winkenwerder on leadership in the military, civilian government, and private sectors. These two seasoned leaders shared insights from nearly a century of experience leading large, complex entities through changing circumstances and crisis situations. Both individuals highlighted the importance of relationships in the direction of complex teams. They stressed the central role of selecting, placing, developing, and caring for high quality people in the formation of high performing organizations. Both speakers illustrated the similarities and differences of leadership in the government and private sectors, and affirmed the central role that values serve in any leadership situation. Additional speakers added depth to the day through the illustration of contemporary and future leadership challenges. CIP/HS Associate Director Mark Troutman provided participants with an overview of the United States and global economy. This background illustrated the challenges of leadership in a resource constrained environment and the complexities of decision-making during time constrained and unique events such as the 2008 financial crisis and its aftermath. CIP/HS Board Member and Dean of Mason's School of Law, Dan Polsby, provided an ethical rounding to the day. He stressed the level of scrutiny that leaders of large and complex organizations live with and the demands of ethical conduct at senior levels. Given the intense visibility of senior positions, ethical conduct must flow from a highly defined framework from within the leader.

CIP/HS Research Fellow Dr. Stephen Prior provided participants an overview of biodefense efforts and the future bioterror threat environment. His presentation centered on the Nunn-Lugar program, which has for the past two decades provided remarkable progress in efforts to control weapons of mass destruction (WMD) and reduce the risk of WMD based terrorism. Nunn-Lugar also serves as an outstanding case study of senior leaders with vision who effect dramatic and peaceful improvements to global security. Workshop participants finished the day with a presentation from Mr. John Monninger (U.S. Nuclear Regulatory Commission) on the Fukushima Daiichi nuclear event of spring 2011. The tsunami conditions off the east coast of Japan, resulting nuclear disaster, and post-incident response called for unprecedented levels of improvisation from the NRC team and its interagency partners. From the start, the team had to constantly learn, adapt, and create structure to meet challenges in its charge to assist the government of Japan in its efforts to mitigate the effects of unforeseen events.

The overarching theme of the leadership seminar was the level of complexity, innovation, and judgment required of leaders in senior positions. Those with the responsibility to create, operate, sustain, and safeguard infrastructure require a unique skill set. Specifically, the workshop revealed that leaders in the infrastructure protection space must develop skills that are:

Interagency: Modern societies achieve efficiencies and expertise by specializing government functions into departments. However, effective infrastructure design, operation, and crisis response require skills that span individual departments and branches of government. Leaders in the infrastructure protection area must be able to form flexible teams and effectively employ representatives from varied departments into a coherent whole. Moreover, leaders must rapidly identify requirements, and quickly form effective control

(Continued on Page 21)

Security Analysis and Risk Management Association (SARMA) Annual Conference

In September 2011, CIP/HS co-hosted and presented at the Security Analysis and Risk Management Association's (SARMA) 5th Annual Conference. The following article, published in the October 2011 issue of *The Risk Communicator*, features some of the main concepts and topics discussed at the event.

Each year, following the conference, *The Risk Communicator* highlights some of the key panel discussions and speeches from the conference. This year, we [SARMA] take a closer look at the U.S. Coast Guard's Maritime Security Risk Analysis Model (MSRAM) program, one of the most dynamic and promising risk assessment tools to emerge since September 11.

Panel Participants: Commander Brady Downs, Deputy Chief, Port Security Evaluations Division, USCG; Jeff Fuller of ABS Consulting; and Mark Lepofsky of Virtual Risk Technology.

Brady Downs, the current Deputy Staff Director of the National Maritime Domain Awareness Coordination Office (as well as a recipient of SARMA's 2011 Edward J. Jopeck Founder's Award), began the presentation by describing MSRAM's evolution out of the Coast Guard's Port Security Risk Assessment Tool (PSRAT) program. PSRAT, which was created after September 11 as a manageable risk management tool, was a good start, CDR Downs explained, but was limited because it kept threat and vulnerability metrics constant and could only generate a consequence-based lists of assets to protect.

MSRAM took this effort a major step forward by focusing on "providing leaders at all levels of command with risk analysis and risk management decision support for all terrorism threats in the maritime domain." The objective, CDR Downs explained, is to be able to support both tactical decisions at the field level and operational and strategic decisions by "rolling up field level risk assessments to portray risk density of targets at the sector, district, area, and headquarters level."

The result is a program that is integrated up and down the level of command. As with other risk assessment models, the threat component is a key element of MSRAM and is done by the Coast Guard Intelligence Coordination Center. But, as Jeff Fuller, Senior Security Risk Analyst at ABS Consulting, noted, the program relies on multiple review levels that use local and area maritime security committees comprised of port partners and Coast Guard sector commanders. This bottom up process, Mr. Fuller explained, gets buy-in at the local level, which makes the program truly effective.

All three participants emphasized the deep technical sophistication of the data set behind MSRAM, which marries detailed risk assessment databases with GIS visualization tools. Beginning in 2006 with 18,862 targets and 16,599 scenarios, MSRAM now contains 28,319 targets and 85,259 scenarios, with each target assessed against standardized attack methods to maintain consistency of analysis (a boat bomb, for instance, is assigned a certain level of equivalent TNT.) This detailed level of data also brings clarity to budgeting issues because any proposed cut to Coast Guard funding can be translated into the amount risk planners will have to accept in exchange.

Dr. Mark Lepovsky, Vice President at Visual Risk Technologies, provided an overview of the key visualization component of MSRAM. Previous efforts, he noted, required "looking at something inherently spatial but looking at it in a spreadsheet." In the MSRAM system, every target type is laid out on a GIS map with an icon colored based on risk risk. A visual system, Dr. Lepovsky noted, solves a number of tabular problems, including errors that would creep in when unconfirmed geographic coordinates were entered into risk management systems. Geospatial mapping also opens up a number of promising avenues, such as evaluating breach stand-off distances for different containers, as well as paths for vessels and barges and the general

(Continued on Page 24)

InfraGard

In Spring 2011, InfraGard's Nations Capital Members Alliance (INCMA), in partnership with CIP/HS, hosted two lectures at Mason's School of Law.

The first event focused on "The Professionalization of Cyber Criminals and Their Evolution into Strategic Adversaries." The speakers were Jessie M. Eisenbart, a Federal Burea of Investigation (FBI) Intelligence Analyst in the Cyber Intelligence Section, National Cyber-Forensics and Training Alliance in Pittsburgh, Pennsylvania; Mark Danner, Consulting Manager with National Strategies, Inc.; and Robert A. Miller, a Professor of Systems Management in the Information Resources Management College at National Defense University.

With their portrayal in the media, cyber criminals are often viewed as derelicts hiding in their mothers' basements, playing video games during the day and committing petty crimes during the night. Many people often forget that cyber criminals are, in fact, criminals. The cyber crime community is a robust global industry and serious cyber crime is becoming dominated by criminals who view themselves as businessmen. To these criminals, dealing with law enforcement is simply a nuisance of their business, to be dealt with as efficiently as possible to maintain their bottom line. The panel described how cyber criminals evolved their practices to make their crimes more profitable, how they expanded their social networks, divide labor, choose specializations, establish reliable communication infrastructures, and organize their crimes. For today's cyber criminals, cyber crime is their chosen profession, not a hobby. Originally, most hackers were individuals or small groups, looking for notoriety and respect, and perhaps a bit of chaos. Early in this century, we moved to a second stage which saw the rise of cyber-criminals, looking primarily for profit. We are now seeing the beginning of a third stage, in which cyber "exploits" are being weaponized, and cyberspace has become a battle space.

The second event focused on "Hurricane Katrina's Strategic Context, Responses and Lessons Relevant to Recent Disasters in Japan and the U.S." The featured speakers were Colonel Robert Stephan, former Assistant Secretary of Homeland Security for Infrastructure Protection and currently Executive Vice President of CRA; and Jim Caverly, currently the Special Advisor to the Assistant Secretary of Infrastructure Protection at DHS. Col. Stephan presented his slides on the extent of the Hurricane Katrina mega-disaster, showing many images that have seldom been seen before by the general public. This event could not be timelier in light of the Japanese mega-disaster in March 2011 that featured an earthquake and aftershocks, a tsunami, flooding, several radiological emergencies, as well as the recent deadly tornados and violent storms that swept through the Southern United States. The Federal government is taking concerns about mega-disasters very seriously and the DHS National Level Exercise 2011 was designed around a massive earthquake in the New Madrid Seismic Zone (NMSZ). Planning for disasters must now assume the likelihood that multiple types of disasters can happen simultaneously. After his presentation, Col. Stephan was joined on a panel by Mr. Jim Caverly, and together they addressed practical ways that public-private partnerships, such as InfraGard, can provide subject-matter experts (SMEs) to DHS, FEMA, other Federal agencies, and State/local emergency responders to better protect critical infrastructure before disaster strikes – and to accelerate the recovery of damaged critical infrastructures after an emergency.

Please visit INCMA's website for more information. ❖

This article was excerpted from INCMA's Lecture Series event website. To read the full announcements, please click here and here.

XSCM – The New Science of Extreme Supply Chain Management: A Workshop at CIP/HS

by Irvin Varkonyi, Adjunct Professor, George Mason University, Transportation Policy Operations and Logistics

In May 2012, a diverse group of private and public sector attendees participated in an interactive workshop, "X-SCM, The New Science of Extreme Supply Chain Management," based on the textbook of the same name to understand how to better manage the critical issue of volatility when delivering goods and services. The event was hosted by CIP/HS and sponsored by local chapters of supply chain related associations. The workshop's general and breakout sessions identified the means to measure, mitigate, and resolve the impact of volatility in our increasingly globalized world.

"X-SCM is being developed into a multi-faceted, multi-media set of products to serve as a definitive guide and toolset for executives who operate global supply chain networks in a period of systemic, extreme change," said Dr. Sandor Boyson, co-author of X-SCM and Co-Director of the University of Maryland's Robert Smith School of Business' Supply Chain Management Center. "Consider the global wild ride of the last few years — a great recession with the collapse of the U.S. housing market and subsequent collapse of housing elsewhere, including Europe; growing war between nations and non-nation states; drastic changes in government in the Middle East and North Africa; and amazing technological change revolutionizing communication and information sharing. Volatility has emerged as a systemic condition; rapid oscillation through extreme contrasts has become a business constant, the 'new norm,'" Boyson said.

A variety of speakers were brought together by the sponsors representing the Virginia/Maryland/DC area:

- Association for Operations Management (APICS)
- American Society of Transportation and Logistics
- Council of Supply Chain Management Professionals
- Institute for Supply Management
- National Association of Purchasing Management
- Supply Chain Council
- Warehouse and Educational Resource Council

Academic sponsors included CIP/HS, University of Maryland Smith School, and the Thunderbird School of Global Management. The sponsor associations came together to demonstrate the impact of volatility as a consistent event affecting their members. The institutions of higher learning identified the changes in globalization which are influencing the direction of academic programs for students in business, supply chain, and homeland security. Corporate sponsor SAIC underwrote the workshop.

Supply Chain Management (SCM) is both understood and misunderstood within the business community and by public sector stakeholders. Dr. Doug Lambert and the Global Supply Chain Forum define SCM "as the integration of key business processes across the supply chain for the purpose of creating value for customers and stakeholders."[1]

Four breakout sessions were featured, which were capped by an exercise on "China, the Nightmare Supply Chain Disaster."

Business Processes and the Impact of Volatility: Hart Rossman (SAIC) and Carlos Alverenga (Accenture)

IT systems are now increasingly volatile and difficult to secure. Globalization and outsourcing have added orders of magnitude of risk to the integration of hardware, software, and networks. Only 20

(Continued on Page 18)

1. Martha C. Cooper, Douglas M. Lambert, and Janus D. Pagh, "Supply Chain Management: More than a New Name for Logistics," *International Journal of Logistics Management*, 8(1), (1997), 1-14.

Supply Chain *(Cont. from 17)*

percent of computer chips used in IT systems nation-wide are produced in America; and more and more code is imported from India and Eastern Europe. A new discipline, cyber supply chain management, combines cybersecurity, risk analysis, and supply chain assurance and is being applied to end-to-end IT systems impacting the landscape of new industry and government initiatives designed to promote cyber-supply chain management.

Traditionally, risk management has not been a principal focus for supply chain, manufacturing, and procurement executives. Today's complex global networks and market volatility are leading high-performance businesses to re-examine the role that finance and risk management play in global operations. These companies are beginning to follow a new approach by incorporating finance and risk management knowledge and skills into day-to-day supply chain management. This new approach treats operational risk with many of the same techniques as financial risk as presented in the X-SCM textbook.

Measuring Risk and Volatility: Taylor Wilkerson (LMI) and Bradley Palmer (Committee of Sponsoring Organizations Enterprise Risk Management Framework)

Risk is present in all of our professional and personal activities. Measuring risk is necessary to manage risk. Knowledge management in risk is important to operations professionals in the private and public sectors. This must also be offered in the context of efficient operations as offered in the APICS Body of Knowledge.

Supply chains are a complex network of companies coordinating in order to process raw materials, produce components, assemble final products, and distribute products to customers. These networks often stretch across the world, across industries, and across cultures. These networks are vulnerable to disruptions from natural disasters, severe weather, labor disputes, political disputes, market disruptions, and malicious actions. These disruptions hinder the ability to bring products to the customer and can result in damaged product, lost sales, and brand loss. Many companies are now taking actions to manage their supply chain risk exposure and have found significant value in doing so. Following basic best practices can help supply chain managers avoid disruption or minimize resulting losses if disasters occur.

Systems' Volatility: Dr. Mark Troutman and Steve Brady (Voluntary InterCommerce Industry Solutions)

The industrial supply chain is global and distributed in a horizontal and vertical fashion. Falling communications and transportation costs allow firms to conduct stages of production in locations best suited to perform work. This paradigm overturns the view that the manufacture of whole goods takes place in locations with the lowest labor costs. Firms realize efficiency gains in this arrangement, but their activity brings new vulnerability considerations. Central to this supply chain is entity resilience, known as continuity of operations (COOP) in government terms and business continuity to private sector firms. Human capital resident in the workforce represents a necessary input to commerce which is impossible to replace in the short-term and difficult to replace in the medium to long-term.

The evolution of supply chain management from individual, non-collaborative business units/silos toward integrated collaborative supply chains has been integral to more productive and efficient supply chains. The impact of such collaboration on systems' volatility is a critical question in today's supply chains.

Supply Chain Disasters and Resilience: Jock Menzies (American Logistics Aid Network) and Debbie van Opstal (U.S. Resilience Project)

We can all remember our feelings of astonishment, bewilderment, and concern when Hurricane Katrina wreaked unimaginable havoc on our country. This national disaster prompted an outpouring of generous donations from caring people and organizations around the country. Unfortunately, those donations could not be distributed efficiently to provide much-needed relief because there was not a system in place to handle a relief effort of

(Continued on Page 23)

Stability Operations Training and Education: James Madison University's Multi-disciplinary Approach to International Stabilization

by Kenneth F. Newbold, Director of Research and Innovation, James Madison University,
Benjamin T. Delp, Associate Director for Research Development, James Madison University, and
Nicholas E. Rau, Doctoral Assistant, Research and Public Service, James Madison University

The Institute for Infrastructure and Information Assurance (IIIA) at James Madison University (JMU) continues to evolve as global challenges emerge and national needs are identified. Over the past two years, JMU has focused much attention and effort toward stability operations in post-conflict zones. This follows a more than 15-year commitment toward international stabilization through the Center for International Stabilization and Recovery (CISR), formerly the Mine Action Information Center, whose longstanding relationship with the U.S. Department of State was recognized by Secretary Hillary Clinton in December 2011. Policies in Iraq and Afghanistan, along with strategic partnerships with senior U.S. officials, provided the opportunity for JMU to build off of the successful CISR program array in order to expand offerings in research, academic programming, and outreach.

The recent initiatives toward stability operations beyond land mine remediation, peer-to-peer support, and victim's assistance can be traced back to JMU Integrated Science and Technology Professor Karim Altaii's Franklin Fellowship with the State Department, where Dr. Altaii served as a Foreign Affairs Expert helping to build capacity in the Iraqi Higher Education system. Dr. Altaii facilitated a visit to JMU by Ambassador Ryan Crocker, who at the time was rotating out of his Ambassadorship to Iraq and had accepted a position at Texas A&M University. Ambassador Crocker, who at the time of this writing serves as the Ambassador to Afghanistan, accepted this invitation and visited JMU in December 2010.

Secretary of State Hillary Rodham Clinton recognized the Center for International Stabilization and Recovery at James Madison University in December 2011 for publishing the tenth annual To Walk the Earth in Safety, the Department of State report on the United States' Conventional Weapons Destruction Program. For the past four years, CISR staff have written, designed and published the journal that exhibits U.S. efforts to destroy conventional weapons stockpiles. Pictured from left to right: Eric Wuestewald, Suzanne Fiederlein, Ken Rutherford, Secretary Clinton, Lois Carter Fay, and Heather Bowers.

Ambassador Crocker's visit to JMU was received with much enthusiasm and excitement from both the JMU and Harrisonburg community. In order to best utilize Mr. Crocker's time on campus, four activities involving diverse audiences were planned: 1) high level briefings on JMU national, homeland, and human security research and academic programs; 2) a roundtable discussion with JMU faculty representing multiple disciplines and colleges; 3) a lecture to JMU students studying international affairs and intelligence analysis; and 4) a public lecture open to the local community. After a day and a half of meetings and robust discussion, Mr. Crocker saw a potential role for JMU in the on-going conflicts

(Continued on Page 20)

JMU *(Cont. from 19)*

in the Middle East, and introduced Vice Provost John Noftsinger to the Special Inspector General for Iraq Reconstruction (SIGIR), Stuart Bowen.

Seizing on this new opportunity in 2011, representatives from JMU held multiple meetings with Mr. Bowen and his staff, both at the SIGIR offices in Crystal City and on campus in Harrisonburg, VA. Mr. Bowen recognized a connection between JMU's Center for International Stabilization and Recovery, the work of Professor Karim Altaii at the State Department, and the unique program array at JMU (especially in Intelligence Analysis and Civil Affairs coursework). The challenges were laid out by SIGIR in *Hard Lessons: The Iraq Reconstruction Experience*, SIGIR's examination of the first five years of the office's efforts to provide oversight of the $50 billion appropriated for reconstruction in Iraq. Goals and objectives focused on how best to utilize JMU's proven capabilities in the field of stability operations, while leveraging the University's reputation as an honest broker among stakeholders.

In late August 2011, JMU made a commitment to examine additional curriculum and degree offerings specific to post-conflict reconstruction and stability operations. Given JMU's previous success in developing both a Civil Affairs and an Intelligence Analysis curriculum, the opportunity was ripe for exploration. From previous discussions with SIGIR, it was clear that a need existed to produce a more knowledgeable and educated stability operations workforce, with particular emphasis placed on critical thinking, intelligence analysis, budgeting procedures, and contracting. Furthermore, a fact finding exercise revealed a relatively small number of post-secondary institutions operating in this space.

Ambassador Ryan Crocker addresses a standing room only crowd at James Madison University.

In order to fully explore the domain of reconstruction and stability operations, a committee consisting of JMU faculty and administrators was convened in September 2011. The committee knew through previous exercises in program development, and given the potentially broad initial landscape of knowledge and skills necessary, that a multi-disciplinary approach to curriculum development was fundamental to program success. Early on in this process, it became evident that the focus for any curriculum within this arena needed to be practitioner-based, with specific attention placed on connecting theory to practice. Using September and the early part of October as working months, sub-committees formed and identified domains that were thought to be essential for both military and civilian program participants.

Through these conversations and working groups, it became clear that while an opportunity to shape innovative curriculum existed, oftentimes within higher education the process of approving a new curriculum and enrolling students can be quite time consuming. This became a challenge in October 2011, when the *Washington Post* reported that 16,000 U.S. civilians were scheduled to remain in Iraq after the impending 2012 removal of U.S. military forces. This created a short-term focus to assist current practitioners, while keeping a long-term goal of developing academic degree programs.

(Continued on Page 22)

Pepperdine *(Cont. from 14)*

structures — often improvised — to achieve synergy. Finally, leaders in the Executive Branch must understand and form relationships with other branches of government — legislative and judicial — to accomplish policy objectives.

Intergovernment: Each of the conference examples required leaders to direct operations and exercise responsibilities with functions found at different levels of government. The distribution of authorities between national, provincial (State), and local levels differs across nations, but all modern societies share this essential complexity. Leaders need to know governing structure and fashion action within the legal bounds of distributed authorities. Resources likewise reside at differing government levels, and leaders must extend their frameworks to bring the right elements to bear at critical times.

Interdisciplinary: Infrastructure protection solutions do not spring from a single source or discipline, such as engineering or finance. Rather, solutions require the formation of multi-specialty teams tailored to meet unique situation requirements. Resolution often forms in the context of political systems, which can affect the composition and timing of solutions.

International: The dramatic advances in transportation and communications of the past century transcend national borders. The result is that both infrastructure protection challenges and solutions seldom reside within the borders of a single nation. In the Fukushima Daiichi example, both the effects of the incident and response efforts quickly became international in scope. To a greater extent than ever before, leaders in the field of infrastructure protection must master diplomatic skills.

Industry-Government: In each case, conference participants illustrated challenges that required leaders to realize outcomes through the combined efforts of industry and governments. These broad groups bring strength thorough their different attributes, but leaders must often exert considerable effort to create the relationships required to realize synergy. Non-profit and charitable entities also have an important role to play. Failure to create an effective working relationship across diverse sectors yields flawed efforts, misplaced or unused resources, and problems that languish unsolved.

An important leadership element involves the relationships that a senior leader brings to the situation and creates through interaction. In many instances, these relationships were minimal or nonexistent going into key decisions or crisis. The complexities inherent in the attributes above can be challenging, and an active program of engagement and exercise is effective in building the teamwork and mutual understanding necessary to realize synergy across sector, specialty, department, levels of government, and borders. Engagement and exercise are also effective in developing the intangible skills that leaders must have to exercise effective judgment at critical times.

In all, the second annual CIP/HS-Pepperdine Leadership Workshop was highly valuable, thought provoking, and provided ample avenues for further study. Such executive education events are low cost, effective ways to identify key concepts and achieve a high level of group learning. A valuable day for all, CIP/HS leadership will look for other such venues to examine the dimensions of leadership in the infrastructure protection community. Leadership in the infrastructure protection area is a subject ripe for development and inclusion into professional education programs. ❖

JMU *(Cont. from 20)*

Additionally, the committee recognized that the domain of reconstruction and stability operations is not limited to conflict zones abroad. Hurricane Katrina, the increased outbreak of tornadoes in the Great Plains States, and flooding along the Mississippi and Missouri Rivers, to name a few, are recent events that have revealed the need for enhanced educational opportunities for first responders and emergency managers operating on U.S. soil.

Special Inspector General for Iraq Reconstruction (SIGIR) Stuart Bowen visits with members of the James Madison University community. Pictured from left to right: John Noftsinger, JMU Vice Provost for Research and Public Service; Ginger Cruz, formerly the Deputy Special Inspector General for Iraq Reconstruction; Karim Altaii, JMU Professor of Integrated Science and Technology; and Stuart Bowen, Special Inspector General for Iraq Reconstruction.

In order to meet this short-term need for education and training, JMU has decided to focus immediate attention toward a conference with clear objectives to foster interagency communication, share education and training strategies, and allow for the free flow of new ideas within the domain of reconstruction and stability operations at an academic, neutral site. By bringing together U.S. military and civilian officials, along with representatives from the private sector, think tanks, NGOs, and academia, this effort, slated for Winter 2012, will afford the many diverse stakeholders in this field the opportunity to flesh out the current state of stability operations, and identify what steps need to be taken to ensure U.S. success in missions abroad.

A natural fit exists between critical infrastructure protection (CIP) and international stabilization, and JMU has linked two premier research centers to apply lessons learned from both perspectives to advance human security initiatives. As with many aspects of CIP, partnerships are crucial to implementing successful solutions. Through expanded international collaboration, new approaches will be discovered that will enhance the reliability and security of our Nation's infrastructure, both at home and abroad. ❖

Supply Chain *(Cont. from 18)*

this magnitude. The need for a central contact point became very evident. Who better to bring order to chaos than members of the logistics profession? To this end, a group of concerned industry professionals teamed up to create the American Logistics Aid Network (ALAN.)

Over the last decade, global enterprises have innovated new supply chain risk management systems that create greater confidence in sourced materials, shipment security, product integrity, and supply chain continuity. These tools and processes can also help to narrow the risk of strategic disruptions to the national supply chain as well as the dangers of a cyber "Trojan Horse." Vendor assessment and audit programs, quality assurance programs, supply chain mapping, use of GPS, and sensor systems are only a few of the best practice examples of business capabilities that can help satisfy both the national supply chain security strategy and the national cybersecurity strategy.

Differences in language and perspective often blur the commonalities of interest between government and industry. For example, government focuses on threats and vulnerabilities while business focuses on managing risks. Government seeks to cope with catastrophic events while business focuses on day-to-day continuity. Government's role is to secure systems integrity of national infrastructure for which no individual business can be held accountable.

China, the Nightmare Supply Chain Disaster: Dr. Sandor Boyson (University of Maryland) and Irvin Varkonyi (Mason School of Public Policy, Transportation Policy Operations and Logistics)

The X-SCM workshop concluded with an exercise on "China, the Nightmare Supply Chain Disaster." Attendees were divided into three roles: Government, Electronics Industry, and Retail Clothing Industry. Based on the findings in the video produced by FM Global, various perspectives were brought to bear by attendees. The findings were dramatic in the realization of the potential impact of a weather related disaster in China's Pearl River Delta. More than half of China's exports to the United States are manufactured in this part of China. The implications of a weather disaster would be far more devastating economically to the United States than the nuclear catastrophe caused by the Japanese earthquake and subsequent tsunami which had significant consequences in the electronics and automotive industries. Preparedness by U.S. business and government was deemed insufficient in the event of a disaster in China's Pearl River Delta. The session's discussions focused on the likelihood of such a disaster and the means to mitigate its negative consequences.

The workshop organizers expect to hold an event in 2013 with topics to be decided. For more information, please contact Irvin Varkonyi at ivarkony@gmu.edu. ❖

TISP *(Cont. from 3)*

on TISP's website at http://www.tisp.org/index.cfm?pid=11824. For more information about the 2013 Critical Infrastructure Symposium, please visit the TISP website at http://www.tisp.org/. For more information about the CIP/HS education program and access to available materials, please visit the CIP/HS website at http://cip.gmu.edu/. ❖

CBEP *(Cont. from 7)*

remote places, using the most unusual means, with the most unlikely partners. This is the heritage of Nunn-Lugar; it should be its future as well." CIP/HS is proud to have contributed to the heritage and is looking forward to playing an active part in that future through the ongoing work at Mason. Twenty years and counting.... ❖

SARMA *(Cont. from 15)*

integration of ship movements to minimize risks.

This article provided on overview of just one of the thought-provoking panels. For more information about the 2011 event, please visit SARAM's website at http://sarma.org/events/pastevents/. An announcement on the 2012 SARMA Conference will be posted this summer. Please visit the CIP/HS website or SARMA's website for upcoming information. ❖

Resilience *(Cont. from 6)*

accepted body of principles and best practices — will emerge and self-organize through the magic of a search engine. The existence of this concept will not solve any problems of itself. It will, however, result in a better understanding of the entire body of work and lead to the identification of seams which will allow us to address these shortcomings before they can be exploited. ❖

PRC *(Cont. from 12)*

individual employee availability is the essential linchpin to the delivery of critical services, rapid recovery, and organizational survival.

CIP/HS, along with Personal Recovery Concepts, solves the personal resilience gap with a program that combines training and testing of individual COOP roles and responsibilities with family preparedness. To learn more about this innovative online program, please contact Mark Troutman, Associate Director of CIP/HS, at (703) 993-4720. ❖

The Center for Infrastructure Protection and Homeland Security (CIP/HS) works in conjunction with James Madison Univerity and seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems, and economic processes supporting the Nation's critical infrastructure. The Center is funded by a grant from the National Institute of Standards and Technology (NIST).

If you would like to be added to the distribution list for *The CIP Report*, please click on this link:
http://listserv.gmu.edu/cgi-bin/wa?SUBED1=cipp-report-l&A=1