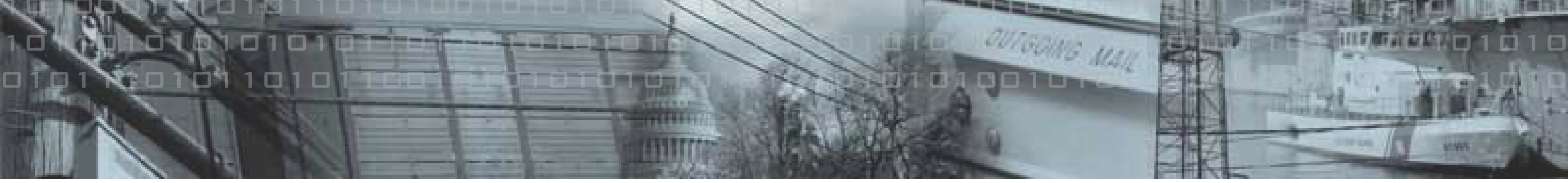


THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION AND HOMELAND SECURITY

NOVEMBER 2013
EDUCATION

EDITORIAL STAFF

EDITOR
Kendal Smith

ASSISTANT EDITOR
Jassandra Nanini

PUBLISHER
Melanie Gutmann

JMU COORDINATORS
Ben Delp
Ken Newbold

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

Follow us on Twitter here
Like us on Facebook here

VOLUME 12 NUMBER 5

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

This month's *CIP Report* focuses on Education. Nothing lasting can be achieved in terms of critical infrastructure security and resilience unless the future workforce understands the operating environment and is fully equipped with both the knowledge and skills to adapt to new situations. Consequently, this issue includes articles emphasizing the need for particular curricular focus, as well as information on specific educational programs and organizations.

First, CIP/HS provides an update on the Critical Infrastructure Higher Education Initiative, a joint project with the U.S. Department of Homeland Security to create and distribute critical infrastructure materials to higher education institutions throughout the United States. Then, West Point faculty Drs. Steven Hart and J. Ledlie Klosky argue for infrastructure as part of a liberal arts education, and Drs. Gary Kessler and Jim Ramsay of Embry-Riddle Aeronautical University consider how to integrate cybersecurity into a homeland security curriculum. Next, we introduce the International Society for Preparedness, Resilience, and Security (INSPRS), an organization devoted to advancing education in homeland security and related disciplines. Angelo State University's Dr. James Phelps then explains why Geographic Information Systems is important for homeland security and emergency management professionals and how it can be taught in an online format. Finally, Benjamin Delp and Amanda Latham discuss James Madison University's critical infrastructure programs, highlighting information technology, intelligence analysis, and emergency services.

We would like to take this opportunity to thank this month's contributors. We truly appreciate your valuable insight.

We hope you enjoy this issue of *The CIP Report* and find it useful and informative. Thank you for your support and feedback.

Mick Kicklighter

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

CIP/HS Update: The Critical Infrastructure Higher Education Initiative

In 2010, the Center for Infrastructure Protection and Homeland Security (CIP/HS) at George Mason University began a partnership with the U.S. Department of Homeland Security's Office of Infrastructure Protection (IP) to create and disseminate higher education programs in critical infrastructure security and resilience (CISR). This "Critical Infrastructure Higher Education Initiative" (CI HEI) brings together public, private, and academic subject matter experts (SMEs) across all sectors to aid in developing courses and materials necessary for a comprehensive approach to homeland security education. All materials are then made publicly available for use in academic institutions across the country.[1]

The initiative began with a four month survey and assessment of existing critical infrastructure (CI) instruction in institutions of higher education throughout the nation. Of the 785 colleges and universities surveyed—including those identified as offering higher education programs in homeland security by the Naval Postgraduate School's Center for Homeland Defense and Security (CHDS)—only 69 courses were found to contain significant CI material. The lack of focus on this subject as well as variations in content and terminology among the proffered courses indicated that robust CISR higher educational materials are needed.

Background

The 2009 National Infrastructure Protection Plan (NIPP) recognizes that a unified and highly skilled workforce is vital for long-term success in securing the nation's critical infrastructure. To that end, the NIPP identifies seven core competency areas needed for effective CI job performance.[2]

To instill these competencies, the NIPP further emphasizes "the development of a long-term higher education program that will include academic degrees and adult education."[3] The importance of such a higher education program lies in

(Continued on Page 3)

(Figure 1, Core Competency Table, Adapted from the 2009 NIPP, p. 84)

Area	Includes Knowledge and Skills To...
Risk Analysis	**• Perform accurate, documented, objective, defensible, transparent, and complete analyses.**
Protective Measures/ Mitigation Strategies	**• Establish CI program goals and objectives based on risk analysis and risk-reduction return on investment.** **• Plan, develop, and implement CI-related projects, measures, and activities. Take advantage of existing emerging and anticipated methods and technologies in order to develop effective strategies, projects, and activities.** **• Implement continuous feedback mechanisms.**
Partnership Building/ Networking	**• Understand the roles and responsibilities of all partners.** **• Establish mechanisms for interacting with partners and exchanging informattion and resources (including best practices).**

[1] All materials can be found at http://cip.gmu.edu/courses/.

[2] *National Infrastructure Protection Plan: Partnering to enhance protection and resiliency* (Washington, D.C.: U.S. Department of Homeland Security (DHS), 2009), 84, accessed November 9, 2013, http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

[3] Ibid., 86.

(Continued from Page 2)

Information Collection & Reporting (Information Sharing)	**• Use systems, tools, and protocols to collect, analyze, organize, report, and evaluate information. • Communicate and share information with sector partners at each tier of governance, including sector-specific, across sectors, and within the private sector.**
Program Management	**• Establish sector-specific or jurisdictional CI goals and plans. • Identify and prioritize CI projects, strategies, and activities for a sector or jurisdiction. • Manage a CI program on schedule, within budget, and in compliance with performance standards. • Design and implement continuous feedback mechanisms at the program level. • Develop and implement CI training plans.**
Metrics & Program Evaluation	**• Define and establish CI metrics based on goals and objectives. • Establish data collection and measurement plans, systems, and tools. • Report findings and conclusions.**
Technical & Tactical Expertise (Sector-Specific)	**Note: This area includes the specialized (sector-specific) expertise required to plan, implement, and evaluate technical and tactical activities, measures, and programs.**

producing CI professionals with capabilities beyond those generally gained through training. Learning occurs on various levels, and while training is useful for developing lower level cognition, it is often less beneficial for building higher level thinking skills. Yet the complexity of the CI operating environment demands professionals capable of higher ordered thought, able to apply knowledge to new situations, synthesize multidisciplinary information, analyze evolving threats, assess risk, and create innovative solutions. Consequently, the goal of the CI HEI is to create CISR materials that will move learners to progressively higher levels of cognition while developing core competency capability.

This is accomplished via educational best practices, the pedagogical methods that are most effective in communicating curricular content. Examples include: clearly stated learning objectives; Learner-Centered Principles; case studies and other authentic, real-world assessments and rubrics; use of technology; different instructional modalities; and flexible grouping practices and cooperative learning. These practices assist in fostering collaboration and strategic problem-solving, preparing learners to analyze risks in a constantly changing threat environment, share information, and view problems multi-dimensionally.

To develop such materials, the CI HEI draws upon SMEs from government, industry, and academia to assist with curricula development, evaluation, and distribution. Roundtables are held to determine course content, evaluate developed syllabi, and suggest outreach and deployment strategies. During the initial roundtables, consensus emerged in three areas that established general curricular design.

First, all courses should be as comprehensive as possible, with each syllabus containing an extensive amount of readings, both fundamental and advanced. This allows individual instructors to adapt to the needs of their particular students and program. The goal is not to furnish SMEs in specific CI sectors, but to begin building a common lexicon and overall operating framework. Specialization can then occur on the institutional level.

Second, much of the initial SME discussion involved accounting for the potential assortment of learner backgrounds in a CI program. Because CI is relevant in so many fields, background knowledge and experience could include areas as diverse as business, emergency management, engineering, intel-

(Continued on Page 4)

(Continued from Page 3)

Derailed: A Case Study of the 2001 Baltimore Howard Street Tunnel Fire with Exercises

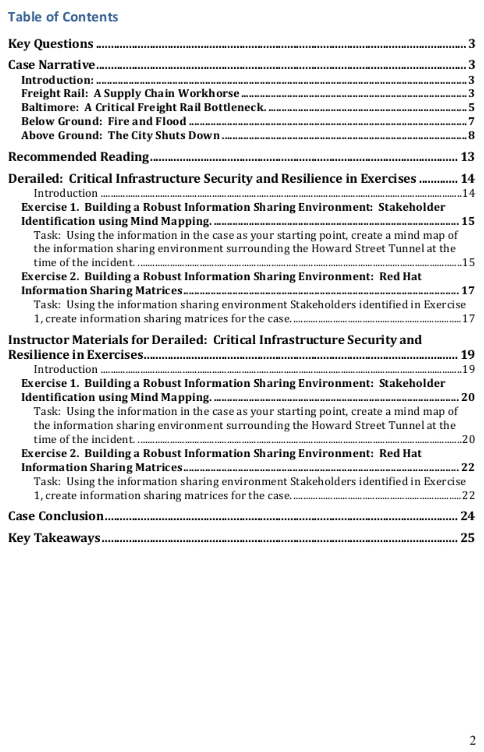


Table of Contents

2

ligence, law enforcement, public administration, or technology—to name a few. Additionally, some learners will already have professional experience, while others will be coming straight from undergraduate study. Background diversity makes it challenging to address the needs of all classroom learners and ensure that each can successfully complete course goals and objectives.

However, it was determined that ultimately the benefits of diversity in the CI learning environment outweigh the challenges. The various perspectives generated in a heterogeneous classroom simulate the reality of a professional community that is inherently interdisciplinary. In such a classroom, a group project or role-playing exercise invites multiple viewpoints and fosters the cross-collaboration essential for the CI profession. CI education *should* reflect this diversity.

Finally, the courses should always balance theory with practical application. Struggling with authentic CISR issues in class is crucial because it enhances critical thinking and provides learners with a genuine awareness of the complexities involved in the field. Hence, CI HEI course syllabi include reflective discussion questions in each lesson, table top exercises simulating CI incidents, and various other activities such as an analysis of interdependencies or the creation of a risk management strategy.

Moreover, the CI HEI has developed three supplemental case studies, complete with exercises and instructor materials. Case studies are a highly effective best practice allowing learners to bridge this gap between theory and application by describing a real-world scenario in which learners use creative problem-solving and adaptive reasoning to generate various solutions. Successful case studies assist in developing the critical thinking skills and analytic tools required in the CISR field and draw upon existing data to demonstrate both successes and failures. Existing case studies focus on the 2007 1-95 Minnesota Bridge Collapse, the 2003 Northeast Blackout, and the 2001 Baltimore Howard Tunnel Street Fire.

Building on this foundation, to date the CI HEI has created twenty-two graduate level CISR courses, includ-

(Continued on Page 5)

*

(Continued from Page 4)

ing nine stand alone courses, a five course certificate program, and an eight course public administration concentration. All materials are substantially reviewed by IP personnel, private sector SMEs, and the academic community before being made available for public use. Courses also undergo a quarterly update to incorporate changes in policy, new readings, recent events, and any additional feedback received.

Outreach

As stated, the CI HEI mission is to create and *disseminate* CISR higher education programs. These materials are not valuable if no one uses them. CIP/HS has thus endeavored to raise awareness through written products; participation in conferences, symposia, and workshops; strategic partnership building; and targeted emails and phone calls.

In addition to articles in *The CIP Report*, CIP/HS has authored a chapter in an upcoming homeland security reference textbook and an editorial for an academic journal that focus on the CI HEI. Such written works not only generate awareness about CI HEI materials, but assist in stimulating conversation among the academic community regarding the need for CI education. The same is true for event participation. CIP/HS has given CI HEI presentations at the Critical Infrastructure Symposium; the Homeland Defense and Security Education Summit; the Transportation Research Board Annual Meeting; the National Military Intelligence Association's Intelligence Education and Training Day; the Security and Risk Management Association's Annual Meeting; and the Association of Contingency Planners DC Chapter Meeting.

Most recently, CIP/HS co-led a workshop with Dr. Steven Hart that focused on overcoming challenges to developing, deploying, and institutionalizing a CI course in each participant's college or university. This type of event is especially useful because even if convinced CI should be in the curriculum and with courses in hand, one must often navigate a quagmire of university obstacles. Are there students to take it? Is there money to fund it? Is anyone qualified to teach it? Assisting faculty in identifying these impediments and generating potential solutions—such as a guiding framework for self-study to prepare a potential instructor[4]—goes a long way towards CI actually being offered in a university classroom.

Also important are partnerships built with key organizations and individuals. For example, in addition to the CIP/HS website, all CI HEI course syllabi and case studies are posted on CHDS' University Agency Partnership Initiative (UAPI) portal, an interactive site where homeland security educators can connect, post events, share materials, and collaborate. UAPI brings together those most concerned with advancing homeland security education and thus provides an excellent forum for promoting CISR as one of its essential elements. Many CI HEI course evaluators and roundtable participants are UAPI members and several have begun utilizing CI HEI materials in their own classrooms. CIP/HS also uses UAPI's directory of homeland security institutions to keep track of relevant programs and send information regarding CI HEI courses.

Conclusion

CI's interdependent nature is an inescapable reality. No one is immune to its failure, and its security involves stakeholders across all levels of government and industry. Despite differences in public/private motivation and regardless of sector expertise, it is vital that all those involved in this process are working with the same lexicon and basic operating framework. The CI HEI has made considerable progress in this endeavor with the creation of comprehensive CISR higher education materials needed to establish a unified professional community capable of securing the nation's critical infrastructure.❖

[4] See Hart, Steven, and James D. Ramsay. "A Guide for Homeland Security Instructors Preparing Physical Critical Infrastructure Protection Courses." Homeland Security Affairs 7, Article 11 (April 2011), available at http://www.hsaj.org/?article=7.1.11.

Infrastructure—A Liberal Art for the 21st Century

by Steven D. Hart, Ph.D. P.E., U.S. Army Engineer Research and Development Center, and J. Ledlie Klosky, Ph.D., P.E., Center for Innovation and Engineering, Department of Civil and Mechanical Engineering, West Point[1]

It is a generally accepted statement that a liberal arts education is focused on those subjects essential for study by a free person to produce well-rounded individuals suitable for citizenship.[2] The history of liberal arts education shows that the 'subjects essential for study by a free person' have evolved over time to meet the changing needs of society. In Ancient Athens, a liberal arts education consisted of grammar, logic, and rhetoric which came to be called the Trivium. The emergence of these skills and the training of youth in their use proved essential to the functioning of the Athenian democracy.[3] Later, in medieval times, the Quadrivium of arithmetic, geometry, music, and astronomy was added to form the seven liberal arts of a medieval university curriculum. These evolved into the contemporary liberal arts of literature, languages, philosophy, history, mathematics, psychology, and science.[4] These are manifested both as the basis for curriculum in 'liberal arts colleges' and in the general education curriculum found in most colleges and universities.

As one would expect, the process of discussion and debate on what constitutes a modern liberal arts education is alive and well within the liberal arts community. In a 1998 speech, W.R. Connor, President of the National Humanities Center, posed the questions, "What does it take to create a truly open, free society in this strange new world we have entered in recent years? What are the skills of freedom today?"[5] In 2003, Jonathan Becker, Dean of International Studies at Bard College addressed *What a Liberal Arts Education is…and is Not* in terms of goals, curriculum, pedagogy, and process, and then in 2009, Harvard President Drew Gilpin Faust, in an address launching Harvard's revised general education program, traced the evolution of Harvard's program through the restructurings of the 1940's and 1970's to the most recent changes. In this speech, she re-validated an idea introduced at Harvard after World War II by stating, "Knowledge should be for citizens, not just for scholars in their disciplines; knowledge should be for responsible human beings and citizens in a democratic society."[6]

We propose that a working knowledge of infrastructure is essential knowledge for citizens in a contemporary, free society and is thus a liberal art for the 21st century.

Right and wrong, sometimes enlightened, and too often foolish, societies are constantly making fateful choices. These choices are more or less deliberate, depending on how that society is organized, and more or less beneficial to that society, other societies, and the environment, depending largely on how well-informed the decision makers

(Continued on Page 7)

[1] The views expressed in this article are the personal views of the authors and do not constitute an official position of the United States Army or Government.

[2] W.R. Conner, "Liberal Arts Education in the Twenty-First Century," AALE Occasional Paper # 2, May 25, 1998, http://www.aale.org/conner.htm; Jonathan Becker, "What a Liberal Arts Education is...and is Not," Modification of a talk of the same title given at the Open Society Institute's Undergraduate Exchange Program Alumni Conference in Budapest, Hungary, June 2003, available in: Bard Essays, Bard Institute for International Liberal Education, http://iile.bard.edu/lib/db_essays.php?action=getfile&id=39897347, 3; Martha J. Kanter, "The Relevance of Liberal Arts to a Prosperous Democracy," Remarks at the Annapolis Group Conference, June 22, 2010, http://www.ed.gov/news/speeches/relevance-liberal-arts-prosperous-democracy-under-secretary-martha-j-kanters-remarks-a.

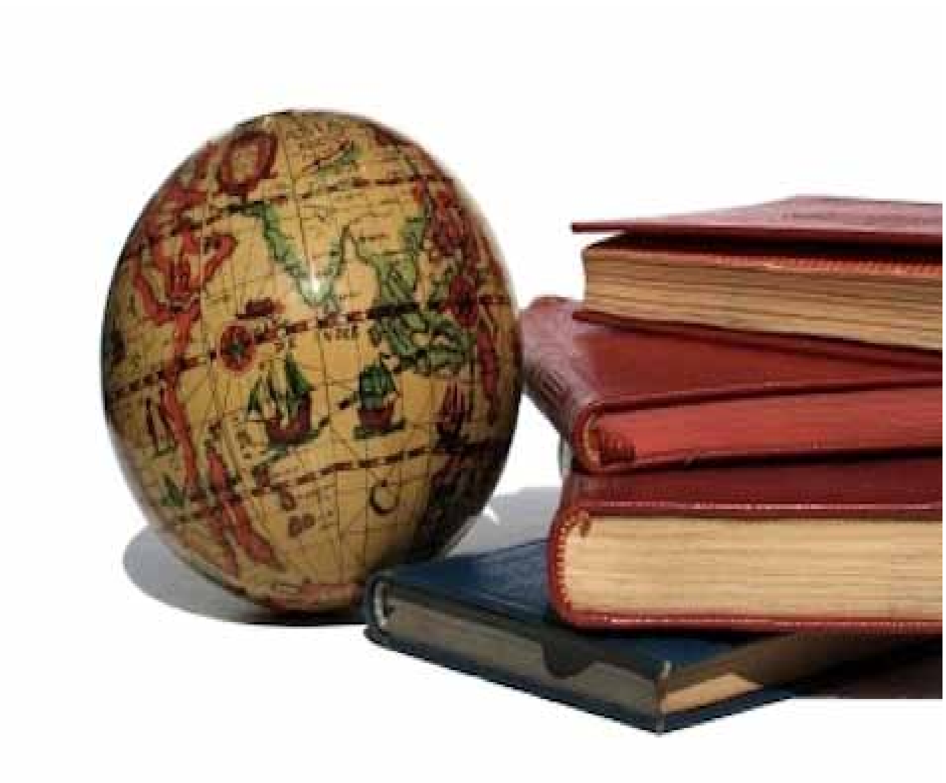
[3] Conner, "Liberal Arts Education."

[4] Marcia Colish. *Medieval Foundations of the Western Intellectual Tradition*: 400-1400 (Yale University Press, 1999).

[5] Conner, "Liberal Arts Education," 7.

[6] Drew Gilpin Faust, "Remarks at the General Education Launch Event," Harvard University, September 3, 2009.

(Continued from Page 6)



are. It is exactly this need for well-informed leaders and voters that justifies including infrastructure in the educational system in the United States.

This cannot be achieved by including infrastructure education for engineers alone and also giving them a smattering of the liberal arts; to educate the citizen needed in a modern technologically-based society, where water, energy, and communications are prominent in the national conversation, a common base of knowledge is needed so that historians, political scientists, philosophers, scientists, and engineers can meet to begin the multidisciplinary, visionary conversations that are essential to answering the most perplexing questions of our times. These conversations will be difficult and time-consuming, but it will require persistent focus across many disciplines to create sustained programs that can provide robust, efficient, and sustainable infrastructure.

For instance, it is not likely to be particularly productive to have an in-depth conversation about electrical power production with someone who does not understand that there is a need for both baseline and peak electrical generation capacity and that excessive demand, insufficient distribution capacity, or under-supply can all lead to the same result. That said, the production of electrical power is an exceptionally important topic, and key questions like “Nuke or not?” need to be discussed if there is to be a rational decision process leading to infrastructure creation that is forward-looking and technically sound. This is not to say that political science or economics majors need to be ready to design a power plant, but they should absolutely be informed actors within the decision process. Conversely, engineers acting alone are equally unlikely to make well-informed decisions about system-level concerns. Sadly, engineers in the past have too-often made decisions that were good for the project or purpose within their purview only to find that the solution had broader societal harms that far outweighed the project gains.

To bridge this knowledge gap, new paradigms are needed which integrate infrastructure as one of the essential elements in the modern graduate’s intellectual development, on par with basic mathematics, writing, and the physical and social sciences. Certainly, if an engineer needs to be able to parse Shakespeare to call herself educated, then a humanities major must possess a basic understanding of where electricity and fresh water come from and where waste goes to call himself educated.

Though it represents only one possible solution, a course intended to fill this need for a multidisciplinary approach to building the infrastructure of our future was described in detail by Hart et al.[7] This course has drawn a surprisingly passionate response from its students, particularly

(Continued on Page 8)

[7] S. Hart, J. Klosky, J. Hanus, K. Meyer, J. Toth, and M. Reese. "An Introduction to Infrastructure for All Disciplines." *Conference Proceedings,* 118th ASEE Annual Conference and Exposition (ASEE, 2011).

(Continued from Page 7)

the humanities majors. For instance, when prompted on a homework assignment late in the course to write about whether they should have been obligated to take the course, students were nearly universally supportive of the requirement and broad in their reasoning:

- "It is imperative that (infrastructure) be taught to all students majoring in American Politics, Comparative Politics and Economics."
- "Regardless of the degree, a working knowledge of infrastructure is vital to being a member of society."
- "A course on infrastructure should be required for all college graduates in order to produce a sustainable society. If we wish to sustain and improve our society… we must understand the systems that underpin it."
- "When more people have an understanding of an issue more valuable debate and dialogue will follow. From this … we can create solutions that make sense."
- "Colleges have a duty to prepare their graduates to be contributing members of society…. I believe that understanding infrastructure is vital to achieving this."
- "Americans must be prepared to anticipate, analyze, and evaluate the state of our continually evolving infrastructure."

Finally, one question on the final exam asked students, "What is the most pressing infrastructure need in the United States today?" One student, a kniesiology major, answered unprompted, "Education—people need to be better educated on what it takes to keep them living the way in which they are accustomed." She then went on to explain how understanding the important concepts of Infrastructure Engineering could lead to changes in societal behavior.

Conclusion

The authors firmly believe that it is absolutely essential that an educated person have a firm understanding of the basic underpinnings of their modern life. This means a grounding in what modern infrastructure consists of and an understanding of how the seemingly disparate infrastructure systems interact to support modern life. By looking at infrastructure in the context of not just technological issues, but also in terms of political, social, and cultural impacts, the student builds a sense of the interconnectedness of political, financial, social, and built systems.

For better or worse, ill-defined problems are the norm in the modern world, and by providing a firm foundational understanding of infrastructure we can learn what the built environment tells us about our past, our future, and the choices we make as a people. Through a firm foundational and shared understanding, it is hoped that technical and non-technical graduates can participate fully in the decision processes that will decide our future. ❖

Cybersecurity Management and Policy: A Vital Component of Homeland Security Education[1]

by Jim Ramsay, Ph.D., and Gary C. Kessler, Ph.D.,
Embry-Riddle Aeronautical University, Daytona Beach, FL*

"Cybersecurity" has emerged as a widely-used buzzword in the homeland security (HS) field today. The fact that all U.S. critical infrastructures[2] are dependent on the flow of reliable data makes information systems vital to the ongoing health of the U.S. economy—and society. Further, these same systems are both aged and vulnerable, making them susceptible to hackers, natural disasters, or terrorists. Cyberattacks today are not just about defacing websites, but instead target specific organizations or industries with an aim of destroying or adversely affecting infrastructure, stealing intellectual property, or disrupting the economy.[3] Complicating matters is the fact that there is a national shortage of cybersecurity expertise.[4]

Cybersecurity concerns affecting U.S. national security seem to be a regularly reoccurring theme. U.S. Secretary of Defense Leon Panetta has warned of an impending "cyber Pearl Harbor."[5] National Security Agency (NSA) Director General Keith B. Alexander publicly asked the attendees of the Defcon hacker conference for their help to secure cyberspace.[6] And the Department of Defense's Cyber Command is slated to quintuple in size in the next several years.[7] Clearly, cybersecurity has entered into the broader realms of national defense and national security. Taken together, it is clear that cybersecurity is on the short list of the national security challenges for the United States. The Clinton, Bush, and Obama Administrations have each recognized the growing importance of securing the U.S. cyberspace and have taken steps to produce plans to do so.[8]

(Continued on Page 10)

[1] Portions of this essay are adapted from an earlier published manuscript. For a more complete treatment of this topic, readers are referred to Gary C. Kessler and James Ramsay, "Paradigms for Cybersecurity Education in a Homeland Security Program," *Journal of Homeland Security Education* 2 (2013), http://www.journalhse.org/v2-kesslerramsay.html.

[2] *National Infrastructure Protection Plan: Partnering to enhance protection and resiliency* (Washington, D.C.: U.S. Department of Homeland Security (DHS), 2009), accessed November 7, 2013, http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

[3] Center for Strategic and International Studies (CSIS) Technology and Public Policy Program, *Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency*, (Washington, D.C.: CSIS, December 2008), accessed November 7, 2013, http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf; "Homeland Security Advisory Council" (HSAC), DHS, accessed November 7, 2013, http://www.dhs.gov/homeland-security-advisory-council-hsac.

[4] Eric Beidel and Stew Magnuson, "Government, Military Face Severe Shortage of Cybersecurity Experts," *National Defense*, August 2011, accessed November 7, 2013, http://www.nationaldefensemagazine.org/archive/2011/August/Pages/Government,MilitaryFaceSevereShortageOfCybersecurityExperts.aspx; Jim Finkle and Noel Randewich, "Experts Warn of Shortage of U.S. Cyber Pros," *Reuters*, June 13, 2012, accessed November 7, 2013, http://www.reuters.com/article/2012/06/13/us-media-tech-summit-symantec-idUSBRE85B1E220120613.

[5] Zachary Fryer-Biggs, "Panetta lays out new cybersecurity policy," *ArmyTimes*, October 12, 2012, accessed November 7, 2013, http://www.armytimes.com/news/2012/10/dn-panetta-new-cyber-policy-101212/.

[6] Lucian Constantin, "NSA Chief Asks Hackers at Defcon for Help Securing Cyberspace," *PCWorld*, July 28, 2012, accessed November 7, 2013, http://www.pcworld.com/article/260007/nsa_chief_asks_hackers_at_defcon_for_help_securing_cyberspace.html.

[7] Ellen Nakashima, "Pentagon to boost cybersecurity force," *Washington Post*, January 27, 2013, accessed November 7, 2013, http://www.washingtonpost.com/world/national-security/pentagon-to-boost-cybersecurity-force/2013/01/19/d87d9dc2-5fec-11e2-b05a-605528f6b712_story.html.

[8] CSIS, *Securing Cyberspace for the 44th Presidency; National Plan for Information Systems Protection, Version 1.0: An Invitation to Dialogue* (Washington, D.C.: The White House, 2000), accessed November 7, 2013, https://www.fas.org/irp/offdocs/pdd/CIP-plan.pdf; *The National Strategy to Secure Cyberspace* (Washington, D.C.: The White House, February 2003), accessed November 7, 2013, http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf; *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington, D.C.: The White House, May 2011), accessed November 7, 2013, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

(Continued from Page 9)

Infusing Academic HS Programs with Principles of Cybersecurity

Academia needs to apply new ways of thinking, new understanding, and new strategies to our nation's response to cyberattacks.[9] Just as cybersecurity is about process rather than technology, our response to cyber-related security challenges are not solely about technical solutions but must also involve myriad related topics such as national defense, economics, sociology, politics, diplomacy, history, and many other social sciences. Over the last decade, academic HS programs have largely arisen as broad, applied social science programs.[10] As such, they are ideally suited to providing a context in which to efficiently place the principles, tools, and concepts required by this new set of professionals charged with managing infrastructures critical to the U.S. economy. Indeed, many scholars have recently observed that such skill sets are desperately needed in government.[11]

The Homeland Security Act of 2002 mandates that academia take an active role in HS education.[12] Cybersecurity education in futherance of DHS' mission and goals is an obvious task. To date, the DHS Science and Technology (S&T) Directorate—the main point-of-contact with the academic community—supports 12 Centers of Excellence through its Office of University Programs. These Centers represent a comprehensive network of universities that develop basic and applied research in science, technology, engineering, and mathematics (STEM) programs that directly support the strategic plan for the S&T directorate and that of the entire DHS. A very real question, though, is whether STEM curricula are the *only* appropriate path for integrating cybersecurity education into the larger HS academic enterprise. STEM-oriented cybersecurity programs are heavily based in computer science and concentrate on programming, tool development, and implementation of security mechanisms rather than the managerial, analytical, or policy components of applied cybersecurity (writ large). In contrast, most (especially undergraduate) HS programs tend to be broad field, applied social science programs that develop the analytical and critical evaluation skills of middle managers. The integration of cybersecurity policy and management aspects in a HS curriculum would specifically address the academic needs of DHS and other HS agencies. Indeed, while a solid foundation in technology is important for those experts in order to detect, respond, and counter-attack in cyberspace, a multidisciplinary approach is also essential for HS professionals.

In particular, rather than attempt to force students into an engineering-based approach to cybersecurity, HS programs should integrate the National Response Framework[13] and, specifically, the all-hazards approach, into a curriculum that fully explores intelligence gathering, threat analysis, planning, management, policy development, risk analysis, and mitigation, as well as anti-/counter-terrorism.[14] These are the subjects in which HS programs concentrate and they are not generally taught in the classical engineering curriculum.

The combination of a cybersecurity curriculum within a more social science-based HS undergraduate

(Continued on Page 11)

[9] G.C. Kessler, "Information Security: New Threats or Familiar Problems?" *IEEE Computer Magazine* 45, no. 2: 59-65 (February 2012).

[10] James D. Ramsay, Daniel Cutrer, and Robert Raffel, "Development of an Outcomes-based, Undergraduate Curriculum in Homeland Security," *Homeland Security Affairs Journal* 6, no. 2 (May 2012), accessed November 7, 2013, http://www.hsaj.org/?article=6.2.4.

[11] Morgan Little, "Executive order on cyber security builds steam amid criticism," *Los Angeles Times Online*, October 2, 2012, accessed November 7, 2013, http://www.latimes.com/news/politics/la-pn-obama-executive-order-cyber-security-20121002,0,6786970.story; Franklin S. Reeder, Daniel Chenok, Karen S. Evans, James A. Lewis, and Alan Paller, *Updating U.S. Federal Cybersecurity Policy and Guidance: Spending Scarce Taxpayer Dollars on Security Programs That Works* (Washington, D.C.: CSIS Technology and Public Policy Program, October 2012), http://csis.org/files/publication/121019_Reeder_A130_Web.pdf.

[12] Homeland Security Act of 2002, Public Law No. 107-296, 6 U.S.C. 188, § 308 (2002).

[13] National Response Framework (Washington, D.C.: DHS, January 2008), accessed November 7, 2013, http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf.

[14] Christopher Bellavita, "Changing Homeland Security: What is Homeland Security?" *Homeland Security Affairs Journal* 4, no. 2 (June 2008), accessed November 7, 2013, http://www.hsaj.org/?fullarticle=4.2.1; Ramsay et al., 2010.

(Continued from Page 10)

curriculum, then, would attempt to bridge the gap between an engineering approach to cyber-security education and the social science approach that aims to address the stated needs of DHS and the changing face of homeland security.[15] This perspective on cybersecurity education is important and timely for HS programs as we have already entered an era of cyberterrorism and cyberwarfare, as evidenced by Advanced Persistent Threat-class attacks, specific attacks on hardware (e.g., Stuxnet and Flame), and attacks on information systems for political and ideological goals (e.g., by groups ranging from Anonymous to the Cyber Fighters of Izz ad-din Al Qassam).

Paradigms of Cybersecurity

Although HS students may not need engineering expertise in order to understand the threats in cyberspace, they do need in-depth cyber-literacy integrated into the balance of their HS education. It is essential that HS students learn real cybersecurity content but at a level consistent with the holistic approach of the core HS program.

Like HS writ large, cybersecurity is not a monolithic discipline. It is a complex and dynamic construct that integrates multiple disciplines. To most people, the term "cybersecurity" conjures up anti-virus software and firewalls. Within the context of a HS program, cybersecurity should comprise multiple dimensions, all of which have a real HS component (Figure 1).

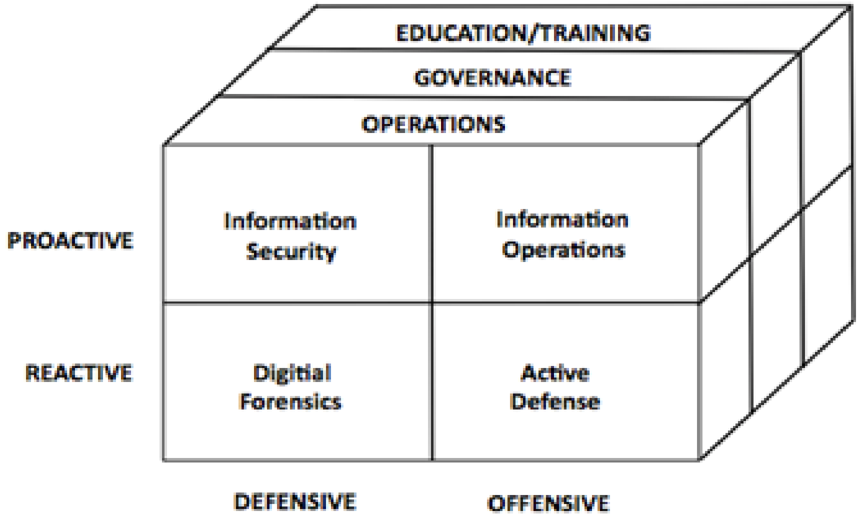


Figure 1. Paradigms in cybersecurity.

First, cybersecurity comprises three planes of study. *Operations* addresses the day-to-day functioning of the information security task, such as staffing, policies and procedures, incident response, business continuity, disaster recovery, systems management, tool acquisition and deployment, and investigations. It is in this plane that an organization needs to identify, assess, and understand its information security needs and select the systems, tools, and technologies required to carry out its mission.

Governance addresses the management of the cybersecurity function, including the development of the organizational structure and command chain that oversees, manages, and handles information and information systems. Roles and responsibilities of individuals in this personnel chain include the chief information officer, chief information security officer, information security administrators and technicians, and data managers.

Education/training addresses knowledge transfer to cybersecurity professionals, organization staff, the user community, and others. *Training*, in this context, refers to teaching individuals specific skills and competencies that are usually task- or project-oriented, whereas education provides individuals with a systemic understanding of a particular discipline. *Training* makes people become quickly functional with a tool or methodology while *education* is the basis for life-long learning, critical thinking, innovation, and subsequent skill acquisition.

Second, cybersecurity actions

(Continued on Page 12)

[15] Christopher Bellavita, "Changing Homeland Security"; Steve Ragan, "DHS Secretary Discusses Cybersecurity Hiring With Advisory Board," *SecurityWeek*, October 3, 2012, accessed November 7, 2013, http://www.securityweek.com/dhs-secretary-discusses-cybersecurity-hiring-advisory-council.

(Continued from Page 11)

can take place in a pair of two-dimensional spaces that include: actions taken in response to events (*reactive*) or in order to cause an event (*proactive*), and actions taken in order to defend or protect (*defensive*) or in order to attack (*offensive*). Given these axes, there are four general categories of cybersecurity education to address across all three planes.

Proactive, defensive actions are those that actively defend information assets from compromise, unauthorized use, or other activity that violates information security policies. *Proactive, offensive* actions are those activities meant to disrupt the information assets of another entity; the military commonly refers to these types of activities as Information Operations. *Reactive, defensive* actions are those taken in response to an information security event. These actions are generally in the realm of some aspect of incident response or digital forensics, which includes the investigation and analysis of computers, software, network hardware, and data traffic. Finally, *reactive, offensive* actions are a response to some sort of event, including understanding the stimulating event (which might or might not be a cybersecurity incident), preparing an appropriate response, and executing the response plan. This so-called active defense posture combines vigilant (some might say, aggressive) protection of assets, identifying –and learning from—adversaries, and neutralizing a threat before it becomes a successful attack.[16]

Conclusions and Future Challenges

Academically, HS degree programs are clearly charged with producing future managers, analysts, and policy makers who can address current and emerging threats to national security. Given the increase in academic HS programs over the past eight years, they are ideally situated to produce thousands of cybersecurity management professionals. Although academic HS programs are relatively new, information security programs have been available since the 1990s. At this time, however, there is no recognized academic accreditation body or agency for either HS or cybersecurity programs, much less any organized plan to address the DHS's stated needs of hiring cybersecurity professionals. This poses a real challenge to the efforts aimed at producing bona fide HS and cybersecurity professionals; the lack of accreditation means that any program can teach whatever it wants, is not compelled to teach specific outcomes, and can still name itself "homeland security." A proper and thorough review by the academic community of the cybersecurity workforce needs of the nation will ultimately require some level of standardization of student learning outcomes that are realized by a recognized accreditation body. ❖

James Ramsay is a Professor of Homeland Security and the Chair of the Department of Security Studies and International Affairs at Embry-Riddle Aeronautical University in Daytona Beach, Florida. He was Homeland Security Program Coordinator from 2006-2013. He is the co-author/editor of Introduction to Homeland Security *(2012) and* Critical Issues in Homeland Security: A Casebook *(2013), and is currently co-editing/authoring* Fundamentals of Environmental Security *(expected 2014). Dr. Ramsay is also one of the co-founders of the International Society for Preparedness, Resilience and Security (INSPRS.org). Jim can be contacted at james.ramsay@erau.edu.*

Gary C. Kessler is an Associate Professor of Homeland Security at Embry-Riddle Aeronautical University in Daytona Beach, Florida, specializing in cybersecurity. He is a Certified Information Systems Security Professional, Certified Computer Examiner, and on the board of directors of the Consortium of Digital Forensic Specialists. Gary is the co-author of two professional texts and over 70 articles and papers, and immediate past editor-in-chief of the Journal of Digital Forensics, Security and Law. *Gary can be contacted at gary.kessler@erau.edu.*

[16] John Reed, "Inside one of U.S. Cyber Command's offensive units," *Foreign Policy: National Security*, October 24, 2012, accessed November 7, 2013, http://killerapps.foreignpolicy.com/posts/2012/10/24/inside_one_of_us_cyber_commands_offensive_units_0.

The International Society for Preparedness, Resilience, and Security Begins Work

Never before in history has the need for efficient and effectively coordinated public preparedness, resilience, and security been so pervasive or immediate in the United States and in the world. Recognizing this need, the International Society for Preparedness, Resilience, and Security (INSPRS…"inspires") announced its official unveiling on September 27 at the 6th Annual Homeland Security and Defense Education Summit. The Summit, held at Hanscom Air Force Base, Burlington, MA, was sponsored by the Naval Postgraduate School's (NPS) Center for Homeland Defense and Security (CHDS) in partnership with Northeastern University, the Department of Homeland Security, the Federal Emergency Management Agency, and the National Guard Homeland Security Institute.

What is INSPRS? It is an organization dedicated to providing a global forum that advances the education and practice of the emergent academic disciplines of homeland security, civil security, public safety, preparedness, resilience, response, and disaster management. Members of INSPRS conduct research, develop and disseminate best practices, and build connections among academics, policy makers, and practitioners.

The initial planning for INSPRS recognized the need for an integration of several related, yet disconnected disciplines, as well as the development of a professional organization with which to facilitate those interdisciplinary efforts. Another goal is to create a repository for and portal of information for interested individuals, institutions, and/or agencies—public or private.

How did INSPRS come about? In May 2013, a group of 15 homeland security educators representing various institutions of higher learning across the United States met at Penn State Harrisburg to form INSPRS. The goal was straightforward—to form a new international organization. Over the summer months, faculty worked on the creation of bylaws, a constitution, membership categories, and a marketing plan. On September 11, 2013, exactly eleven years post 9-11, the group filed official documents in Pennsylvania for incorporation as a 501(c)3 nonprofit organization.

Many homeland security educators and organizations are already supporting INSPRS. Tom Arminio, a faculty member of Penn State Harrisburg and a founding board member, offered these thoughts:

> I have been involved with anti-terrorism and force protection efforts and emergency management and homeland security in one way or another since the attack on the *USS Cole* on October 12, 2000. I am continually amazed at the depth and breadth of the homeland security enterprise. I am constantly learning . . . . I hope all of us are constantly learning. No one person can claim to be an expert on every aspect of homeland security or homeland defense. But INSPRS will help all of us move forward in a more collaborative, networked, and focused manner with the goal of integrating theory, education, analysis, and practice to help us better understand public safety and societal resilience. I'm excited about the challenges that lay before us and look forward to working with a number of new colleagues to ensure INSPRS has a significant and positive impact on our discipline.

Irmak Renda-Tenali, Program Director, Associate Professor of Homeland Security and Emergency Management Graduate Degree Programs at the University of Maryland University College and editor-in chief of the *Journal of Homeland Security and Emergency Management* (JHSEM) stated,"The establishment of INSPRS is a great relief for the adult education community. As the paradigm is shifting towards a competency-based education model, INSPRS

(Continued on Page 14)

(Continued from Page 13)

will serve as a gathering place where there is that dialogue between academia and the practitioner community. It will help flesh out the competencies employers will seek in protecting our nation's critical assets and making our communities safer and secure. INSPRS will be our beacon."

Steve Recca, Co-Director of CHDS' University and Agency Partnership Initiative agreed, emphasizing the organizations' collaborative potential:

> As Homeland Security education has evolved, there have been useful—and successful 'injects' from the federal government (NPS' CHDS, the U.S. Northern Command-sponsored Homeland Security and Defense Education Consortium (HSDEC), and the George Mason Law School's critical infrastructure project come to mind) and many creative efforts from individual schools. What has been lacking is a coherent, sustained, and *university-led* collaborative agenda to shape Homeland Security education. INSPRS appears ready to fill that gap. The Society builds on past experiences (including HSDEC and its successor, HSDECA) to form a broad 'coalition of the willing' of faculty and administrators deeply immersed in HS theory and practice. INSPRS seems an appropriate and timely vehicle to provide context to, as well as shape and mature the broad Homeland Security academic discipline.

According to Jim Ramsay, professor and Coordinator of the Homeland Security Program at Embry-Riddle Aeronautical University in Florida:

> INSPRS is about the future of preparedness, resilience and security education, policy analysis, and professional development. The last 8 years has shown us that HS and similar programs are increasing in popularity and in number, from 10-15 in 2006 to over 400 today. The time is right to take the next steps in framing the larger notion of HS as a bona fide profession. No other organization exists whose mission is to bridge education standards in these disciplines with research-based policy analysis and development, professional education, student development, and networking. When you consider that INPSRS is already affiliated with top journals such as JHSEM and JHSE, and the nation's leading student honor society (Order of the Sword & Shield), the opportunities students, scholars, and educators have to advance their profession through research and analysis and education is unprecedented. Maybe most importantly, INSPRS offers amazing opportunities for scholars, educators, practitioners, and students to work together to influence the education landscape, eliminate spurious programs, contribute to the body of knowledge, and to guide policy development in order to create a future supply of professionals that are matched to wicked problems facing the U.S., who will maintain liberty and protect the free flow of people and commerce.

INSPRS offers various membership categories to include student memberships, individual members, associate members, and institutional memberships for academic institutions, government, or nonprofit organizations. Individuals and organizations who join between now and December 31, 2013 will get free membership through December 31, 2014. Yes, a year of free membership. Please go to www.INSPRS.org to sign up and to read more about this exciting new international society. While the initial work creating this society has been accomplished, there are many opportunities for interested professionals to become actively involved in INSPRS. We welcome new members. ❖

Teaching Software Intensive GIS Courses to Online Emergency Management and Homeland Security Students

by James Phelps, Ph.D., Assistant Professor, Angelo State University*

Smart phones, tablet computers, digital cameras, and GPS mapping tools are pervasive in many countries. Where there is a cell phone tower there are people with smart devices using mapping technology to change their lives and perspective of the world around them. No effort to develop critical infrastructure protection plans anywhere in the world would be complete without the use of maps. The technology available today in hand-held devices has changed our world in innumerable ways but especially in how we respond to and recover from disasters, protect communities and infrastructure, and plan mitigation strategies from the all-hazards perspective.

When computer-based mapping was initially made widely available, a number of new articles and texts entered the literature describing best practices for teaching geographic information systems (GIS).[1] With the advent of ready access to an ever more capable Internet and the associated ability for more layered mapping capabilities, another wave of literature was published.[2] However, following publication of the 9/11 Commission Report and the lessons from Hurricane Katrina in 2005, there was a shift from teaching GIS to mapping professionals to teaching GIS for emergency managers and for disaster/population modeling.[3] Today one of the most pervasive uses of GIS technology is the evaluation of critical infrastructure vulnerabilities and development of critical infrastructure protection plans.

Those who are most involved in post-disaster response and recovery efforts are not the technicians who helped to develop the plans for critical infrastructure protection, but first responders or political managers with little to no knowledge of or ability to use GIS technology. These leaders during disasters do not need to be GIS technicians nor utilizers of the associated software to do their jobs, but do require a fundamental grasp of what GIS technology can provide them if they are to be effective during a response situation. In an effort to reach future political leaders and emergency managers, it is essential to incorporate fundamental GIS into education focused at those who will enter the arena as on-scene leaders, city managers, and local emergency managers. This necessitates a coordinated effort to take software intensive courses and make them available to those without a background in geography, cartography, information technology, or software development and manipulation. These present and future leaders do not have to maintain currency with GIS technology, but do need to know the fundamental functioning of GIS software for them to be able to "ask the right questions" of those who support response and recovery efforts. Unfortunately, virtually all

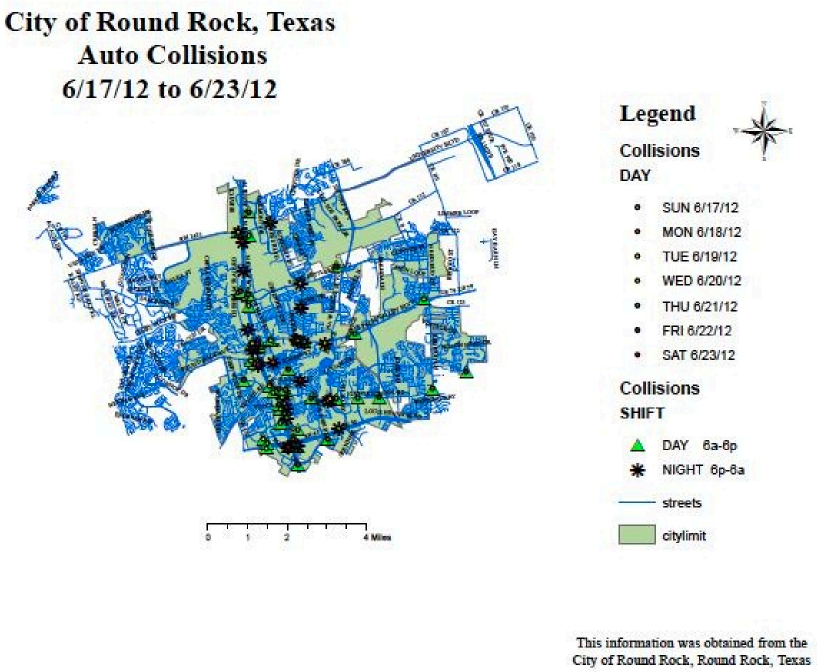
(Continued on Page 16)

[1] There are a large number of articles published at this time. Some of them follow. See Unwin et. al. (1990). A Syllabus for Teaching Geographical Information Systems. *International Journal of Geographical Information Systems*, 4(4), 457-465; Jenkins, A. (1991). Through a Model Darkly: An Educational Postscript. *Cartographica: The international for Geographic Information and Geovisualization*, 28(3), 103-108; Kemp, Goodchild, & Dodson. (1992). Teaching GIS in Geography. *The Professional Geographer*, 44(2), 81-191; Warren, S. (1995). Teaching GIS as a Socially Constructed Technology. *Cartography and Geographic Information Systems*, 22(1), 70-77.

[2] This is just a sampling of the articles produced on teaching GIS using the Internet. See Chen, X. (1998). Integrating GIS Education with Training: A Project-Oriented Approach. *Journal of Geography*, 97(6), 261-268; Easa, Li, & Shi. (1998). GIS Technology for Civil Engineering Education. *Journal of Professional Issues in Engineering Education and Practice*, 124(2), 40-47; Deadman, Hall, Bain, Elliot & Dudycha. (2000). Interactive GIS Instruction Using a Multimedia Classroom. *Journal of Geography in Higher Education*, 24(3), 365-380.

[3] See Carver, Evans, & Kingston. (2004). Developing and Testing an Online Tool for Teaching GIS Concepts Applied to Spatial Decision-making. *Journal of Geography in Higher Education*, 28(3), 425-438; Drennon, C. (2005). Teaching Geographic Information Systems in a Problem-Based Learning Environment. *Journal of Geography in Higher Education*, 29(3), 385-402; Detwiler, J. E. (2008). Comparing student performance in online and blended sections of a GIS programming class. *Transactions in GIS*, 12(1), 131-144.

(Continued from Page 15)



This information was obtained from the City of Round Rock, Round Rock, Texas

Student Project Map #1

current education programs in GIS are based on awarding certifications to technicians or developing modern day computer cartographers with professional degrees.

Recognizing this need, the goal of teaching GIS to first responders, incident commanders, and local or regional emergency managers is not to turn them into geographers, but to make them aware of fundamental benefits certain maps can offer. These benefits range from population demographics where there are flood-prone streets and washes to locations of industrial chemicals and the proximity of schools coupled with current wind and weather patterns. These are just some of the immediate needs that vary with a constantly changing world and the unique situations that local weather, local transportation infrastructure, local manufacturing facilities, and any number of vulnerabilities and threats pose to their communities and populations, as unique to each situation as individual fingerprints are to people.

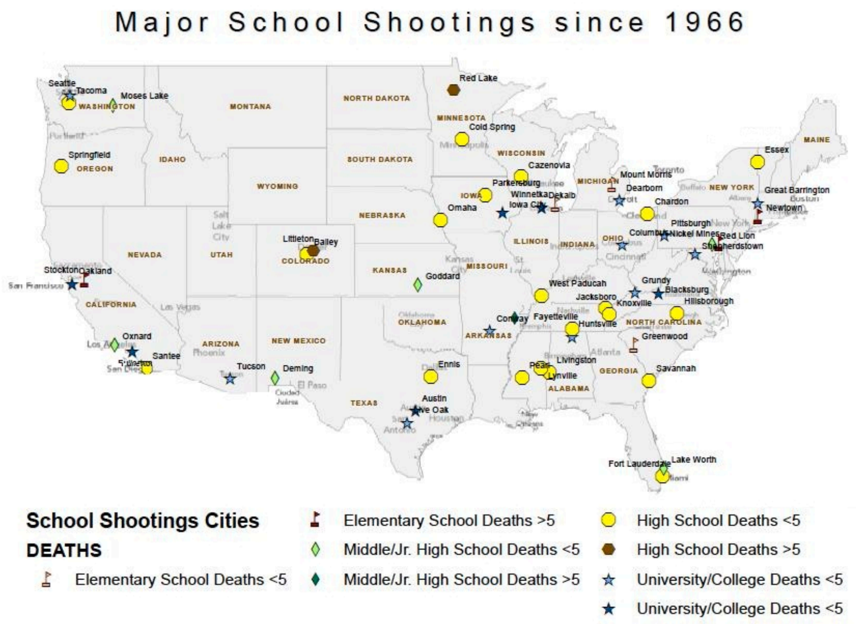
An additional concern in teaching GIS fundamentals to these on scene and local leaders is that the nature of their occupations often preclude them attending traditional on-campus courses. Moreover, traditional social or political science-oriented GIS courses have little applicability to developing comprehension of GIS capabilities in hazard recognition, mitigation, disaster response and recovery, or in critical infrastructure protection. These are unique situations not normally addressed by geography and social science, geological science, or even business education programs. Here enters the Homeland Security and Emergency Management education programs debuting around our country.

Herein lies the problem—the same first responders, incident commanders, and emergency managers who cannot attend traditional university courses, also cannot attend most Homeland Security or Emergency Management degree-oriented programs. This necessitates that classes be delivered to students in an efficient manner, using the Internet and offering classes online! Yet teaching software intensive courses online in an asynchronous learning environment essential to the nature of these leader's occupations is a nearly insurmountable task for most universities. In a search of online GIS courses for Homeland Security, the top hits were Penn State, Towson, Northern Illinois, George Mason, Northeastern, Miami, and Lehigh Carbon Community College. There are other schools offering online courses in GIS, most directed towards public policy or public administration. Of the Homeland Security online GIS courses at the aforementioned schools, all (except Lehigh's Associates Certificate in GIS) were graduate programs offered by the Geography, Computer Science, or continuing professional education departments, or certificate programs oriented at a wide range of topics unrelated specifically to Homeland Security or Emergency Management.[4]

(Continued on Page 17)

[4] This quick search was conducted using Google and only the first three pages of returns were evaluated. At that point the programs were duplicating or without direct relevance to the search keywords. (Author, 5 November 2013).

(Continued from Page 16)

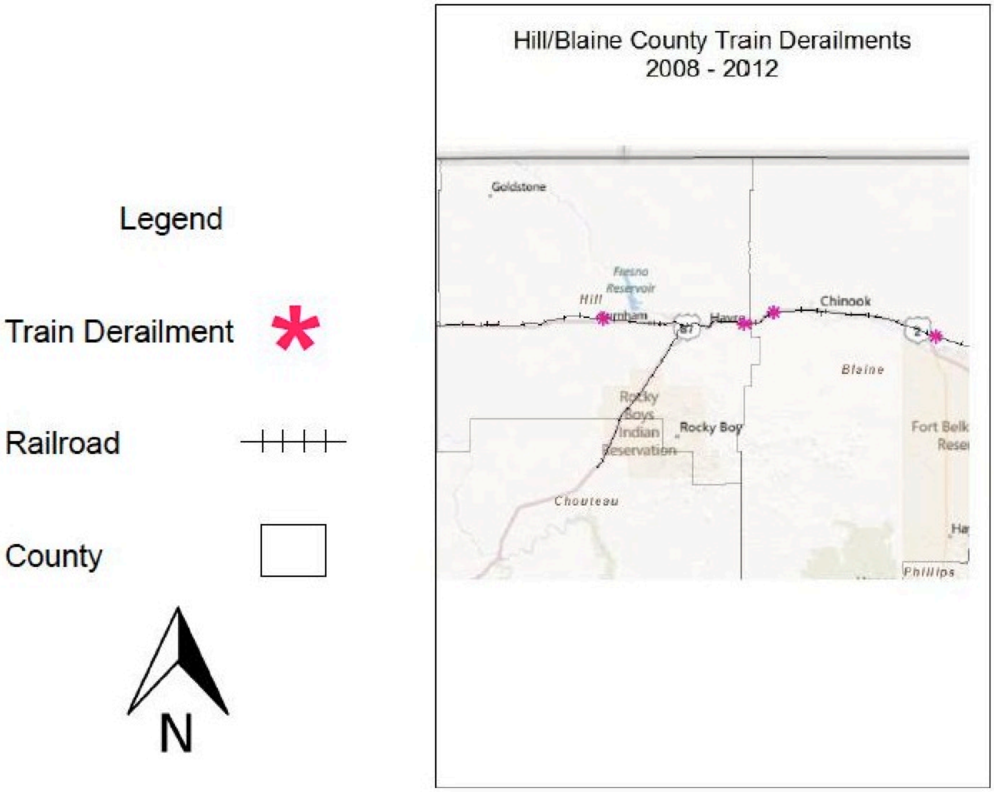


Student Project Map #2

Homeland Security and Emergency Management professionals do not require an extensive background in various software manipulations or five prerequisite courses at the graduate level to reach the point of qualification to take a disaster response or public health-oriented GIS course. What they need is a direct, focused introduction to the benefits offered by GIS software and mapping technology specifically geared towards their occupational field. FEMA offers IS-922, Applications of GIS for Emergency Management, as an online self-paced course to expose emergency managers to the benefits of GIS technology.[5] FEMA also offers in-residence courses at the Emergency Management Institute (EMI), the most applicable for Homeland Security and Emergency Management leadership being E0190, ArcGIS for Emergency Managers.[6] Unfortunately, not all Emergency Managers, professional or political, can attend this course.

At Angelo State University the need for fundamental GIS education and awareness for Homeland Security and Emergency Management professionals was identified at the inception of the Master of Science in Homeland Security degree program in 2010. A required course was developed for graduate students with the intent of introducing them to fundamental GIS capabilities that directly applied to their professional field. This course was expanded to incorporate M.S. in Criminal

(Continued on Page 18)

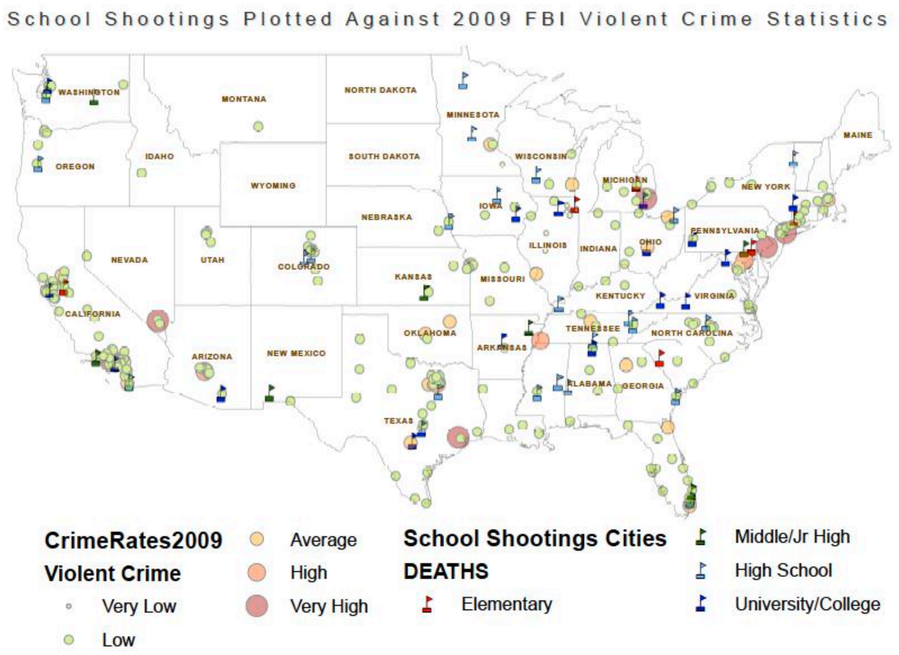


Student Project Map #3

[5] FEMA. (2012). IS-922: Applications of GIS for Emergency Management, available at: http://training.fema.gov/EMIWeb/IS/courseOverview.aspx?code=is-922.

[6] Emergency Management Institute, *Fiscal Year 2014 Training Catalog*, 56.

(Continued from Page 17)



Student Project Map #4

Justice students to familiarize them with the research potential offered by GIS software. A professional geographer with a Ph.D. in the field and associated professional certifications was hired to develop and teach the course. In the initial offering of the course during the spring 2012 semester, a number of deficiencies in design and delivery, as well as deficiencies in instructional methodology, were identified. This resulted in a complete course revision, from basic instructional techniques to software and data set availability.

After experiencing the course as developed by a geographer whose background in teaching included graduate business courses and undergraduate geology courses in a traditional classroom setting, it was determined that a full-time faculty member in the Homeland Security program would need to revise the existing course and instruct the next course offering. As the head of the program at that time and not being one to re-invent the wheel, the determination was made to send me to EMI's E0190 to learn fundamental GIS techniques and use the experience to recreate the course for our graduate students. Attending the in-residence course in the fall of 2012 exposed me to the capabilities of ArcGIS as well as to the damage of hurricane Sandy, a combination of events that allowed real-time application of the fundamental skills learned in E0190 to practical analysis of flooding dangers in Emmitsburg.

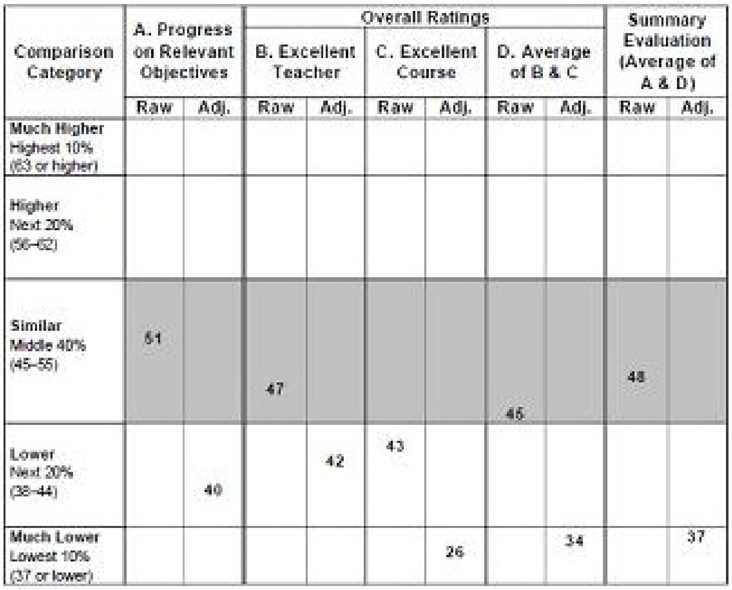
Taking the lessons, student manual, and data sets provided by FEMA, I set out to convert the EMI course to an online, asynchronous format that could be offered to our online graduate students. The original 16 week course developed by the geographer was compressed to 8 weeks. Esri provided ArcGIS 10.1 software for students to download from their site, free of charge. The data sets, practical exercises, and power points used in the E0190 course were recreated as videos and downloadable .pdf and .mdb documents specifically geared to online professional students.

The course was repeated January–March 2013 for a new set of graduate students. After completing all the practical exercises incorporated into the course materials, students were assigned an individual research project to examine a homeland security, emergency management, or critical infrastructure protection project of their own choosing, based on their current residence, and applicable to their local or regional area. Some of their project maps are included here. A requirement of the final assignment (and all course assignments) was to upload the project as a .pdf to reduce the file size, particularly considering the amount of data image files typically contain. Students were also required to submit their metadata for the development of their projects, resulting in some papers running to 190 pages. None of these students had previous exposure to GIS software and all mapping development was based on what they learned from the course. None of the maps are perfect but all are understandable and the experience opened a number of new research opportunities for the students. One student, a professional airline pilot and U.S. Air Force reserve Colonel, is using the skills learned to assist the FAA in updating flight maps. Another student received a graduate research

(Continued on Page 19)

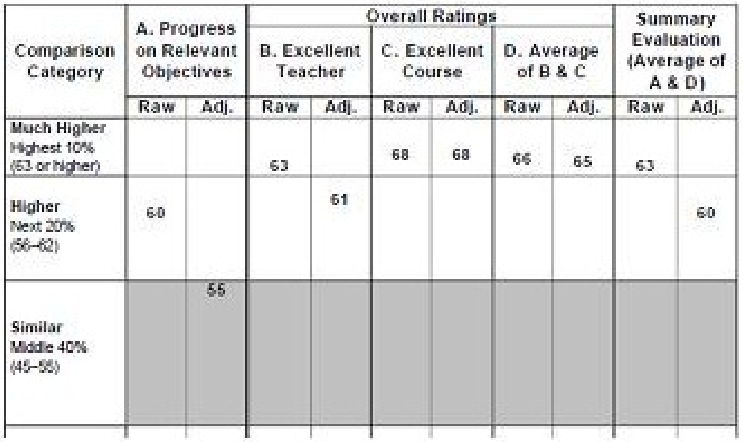
(Continued from Page 18)

Spring 2012



Comparison Category	A. Progress on Relevant Objectives		Overall Ratings B. Excellent Teacher		C. Excellent Course		D. Average of B & C		Summary Evaluation (Average of A & D)	
	Raw	Adj.	Raw	Adj.	Raw	Adj.	Raw	Adj.	Raw	Adj.
Much Higher Highest 10% (63 or higher)										
Higher Next 20% (56–62)										
Similar Middle 40% (45–55)	51		47				46		48	
Lower Next 20% (38–44)		40		42	43					
Much Lower Lowest 10% (37 or lower)						26		34		37

Spring 2013



Comparison Category	A. Progress on Relevant Objectives		Overall Ratings B. Excellent Teacher		C. Excellent Course		D. Average of B & C		Summary Evaluation (Average of A & D)	
	Raw	Adj.	Raw	Adj.	Raw	Adj.	Raw	Adj.	Raw	Adj.
Much Higher Highest 10% (63 or higher)			63		68	68	66	65	63	
Higher Next 20% (56–62)	60			61						60
Similar Middle 40% (45–55)		55								

Figure 1: Course Comparisons

grant and is developing a 10 year study of wildfires in the 14-county region around Austin, Texas. Other students have utilized their skills in follow-on courses as they work towards completing their degrees.

With equivalent numbers of students in the spring 2012 and 2013 courses, and with similar ranges of student backgrounds, the two courses saw a significant difference in student perspective of the material, learning experience, and instructional techniques. The results were notably different from the initial, geographer-developed course as evidenced by student responses on their IEA evaluations of the faculty and the course (Fig. 1).

The spring 2013 course is currently being revised to incorporate some recommended alterations, including improved video presentations. It will be repeated in Spring 2014 and the results will be evaluated to determine if additional revisions are necessary.

Maps are essential to Homeland Security, in all its iterations. First responders and managers do not have to become GIS technicians to benefit from knowledge of the capabilities of GIS software. When working to protect critical infrastructure, respond to disasters, or mitigate losses from future events, a map is worth more than a thousand words. Educating today's Homeland Security and Emergency Management professionals in the uses and benefits of mapping technology is an essential component of higher education programs. Courses need not result in professional GIS certification, but must be established in an easily reachable and simply understandable venue that utilizes known successful teaching approaches. ❖

Dr. James Phelps is the developer of the Homeland and Border Security programs at Angelo State University in San Angelo, TX. A disabled veteran and retired Navy Senior Chief Machinist's Mate (Submarines), he also served as Nuclear Repair Officer and Assistant Radiological Controls Officer in Guam and Hawaii, and has responded to natural disasters ranging from volcanic eruptions to earthquakes, from super typhoons to tsunamis, including a number of nuclear and radiological incidents. Dr. Phelps has developed critical infrastructure plans for military installations, utility systems, and hospitals. His students have conducted directed research developing hospital emergency water supply plans and regional wildfire mitigation programs. He can be contacted at james.phelps@angelo.edu.

James Madison University Critical Infrastructure Protection Education Programs

by Benjamin T. Delp, Associate Director of Research Development, and Amanda E. Latham
Graduate Assistant, Office of Research and Scholarship, James Madison University

James Madison University (JMU) is a community committed to preparing students to be educated and enlightened citizens who lead productive and meaningful lives. This mission engenders a university-wide propensity to engage with the national, homeland, and human security communities in order to develop education, training, research, and outreach programs that address current and future challenges. JMU's responsiveness to national security issues produces a number of deliverables, including academic degree programs, centers and institutes, cutting-edge research, and strategic alliances with private sector, governmental, and educational partners. This overview will concentrate on JMU educational programming focused on the following critical infrastructure sectors (though it should be noted that JMU's CIP-related efforts reach virtually every sector): Information Technology (IT), Defense Industrial Base (intelligence analysis), and Emergency Services.

Information Technology

The Master's Degree in Computer Science Concentration in Information Security program began enrolling students in 1997, and was one of the original seven National Centers of Academic Excellence in Information Assurance Education. The program is 100 percent Internet-based and is delivered through asynchronous interactive classrooms, allowing worldwide access to courses at any time. The program is attuned to the rapid advances in the IT Sector and incorporates new technologies and laws into the curriculum. A funding award from the National Science Foundation Federal Cyber Service: Scholarship for Service program supports several full-ride scholarships, tuition, books, and a stipend for students.

A second concentration in Digital Forensics came online in 2011 in order to provide students with an in-depth, technical study of digital forensics. The curriculum is highly system-oriented, where students gain deep insights into how operating systems, networks, and computer programs function, and how those systems relate to forensics and security in general. Coupled with these technical computer science topics, a core digital forensics component addresses the forensic process, relevant laws, analysis techniques, as well as report writing. Technical forensics topics include digital evidence acquisition, in-depth file system analysis and data recovery, data carving, incident analysis and evidence correlation, memory forensics, network capture and analysis, as well as small-scale device forensic acquisition and analysis.

(Continued on Page 21)

(Continued from Page 20)

Defense Industrial Base (Intelligence Analysis)

Now in its seventh year, the Intelligence Analysis Bachelor of Science (IA) program was designed specifically for students who seek a career as an intelligence analyst, either in the U.S. government or the private sector. IA students learn innovative ways to structure their thinking to solve complex real-world problems when there is both time pressure and a lack of reliable information. A unique characteristic of the program is the integration of coursework that is both technical (data mining, visualization methods, system dynamics modeling) and cognitive (counterfactual reasoning, hypothesis testing, causal analysis). A focus on methods provides students with timeless skills to influence a changing world, including:

- Cognitive Skills: *how to think and reason rigorously*;

- Computational Skills: *how to employ relevant technologies effectively;*

- Communicative Skills: *how to express conclusions in compelling verbal and written products;*

- Contextual Skills: *how to locate conclusions in the broader circumstances in which they occur.*

More than 100 IA graduates are employed throughout the Intelligence Community, U.S. Armed Forces, law enforcement agencies, and industry. Additionally, partnerships supporting research, conferences, internships, and curriculum development have been established with government agencies and the private sector, and include: the Defense Intelligence Agency, the Drug Enforcement Administration, SAIC, and the International Five Eyes Analytic Training Initiative. In order to meet the growing demand for highly educated intelligence analysts, an effort to expand the program is currently underway, which will double the size of the cohorts from 25 to 50 by 2015.

Emergency Services

Integrated Science and Technology Professor Ronald Raab leads JMU's emergency preparedness academic program efforts by offering an array of courses for students, in addition to hosting exercises and trainings for regional first responders. Dr. Raab augments his more than 15 years of experience in the biotech industry with annual trips to FEMA's Center for Domestic Preparedness (CDP) in Anniston, Alabama to complete new trainings. Dr. Raab has taught more than 70 courses and 1,470 emergency responders, which has earned him Gold Trainer status in the CDP's Indirect Training Program. Training highlights from 2013 include:

- Standardized training for all three shifts of the Staunton Fire Department in WMD awareness and setting up emergency response teams;

- Training for the Virginia National Guard 34th Civil Support Team on the topic of homemade explosives; and

- Training for Harrisonburg Rescue Squad in WMDs and HAZMAT response.

Two emergency preparedness courses are offered through the Department of Integrated Science and Technology. All Hazards Response and Management Systems is co-taught by Dr. Raab and retired

(Continued on Page 22)

(Continued from Page 21)

Rockingham County Fire Chief Robbie Symons. The course exposes students to the guiding principles underlying government management systems, and utilizes case studies illustrating the various systems in use. Upon course completion, students receive FEMA certifications in the National Incident Management System (NIMS), the National Response Framework (NRF), and Incident Command Systems (ICS) 100, 200, 300 and 400. The second course, Awareness and Understanding of Chemical, Biological, and Radiological Weapons of Mass Destruction, focuses on the acronym SMELT (Science, Medical, Educational, Logistics, and Tactics) in regards to chemical, radiological, and biological threat agents. Students study the development of vaccines and therapeutic and diagnostic drugs used in the detection and treatment of these agents. Both classes draw students from a variety of backgrounds and majors.

Future emergency preparedness efforts include a course designed specifically for students studying in the Nursing Department. Emeregency Response Training for Health Care Providers will debut in spring 2014. Students will gain knowledge and skills in multiple emergency response situations as well as have the opportunity to earn certificates from FEMA, including Hospital Emergency Department Management of Radiation Accidents and Hospital Emergency Response Training for Mass Casualty Incidents. Additionally, Dr. Raab is leading a collaborative effort between JMU and the Rockingham Memorial Hospital to create an emergency response team based on FEMA's Healthcare Leadership for Mass Casualty Incidents (HCL) training course. HCL introduces healthcare professionals to crucial knowledge and processes involved in the fast-paced decision making that occurs during disasters involving mass casualties.

Conclusion

October saw the one year anniversary of Hurricane Sandy, which should serve as a stark reminder that critical infrastructure sectors are constantly under attack. The threat posed by natural disaster events, accidents, and the malicious targeting of critical infrastructure will continue to rise, following the proliferation of interconnectedness among critical infrastructure systems and national economies. The authors applaud the Center for Infrastructure Protection and Homeland Security's decision to address this timely topic, especially as the Obama Administration moves closer to establishing a new Cybersecurity Framework and Congress debates comprehensive cybersecurity policy reform. The importance of placing a spotlight on CIP education programs that take into account industry trends, social implications, ever-increasing technological advancements, and lifelong learning and professional development cannot be overstated. ❖

The Center for Infrastructure Protection and Homeland Security (CIP/HS) works in conjunction with James Madison University 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