THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION VOLUME 7 NUMBER 6

DECEMBER 2008
CIP UPDATE

Contact: CIPP02@gmu.edu
703.993.4840

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

This month, *The CIP Report* takes a look at some of the projects The Center for Infrastructure Protection (CIP) at George Mason University has underway. There are many new endeavors and ideas that have come about in the past months and we are pleased to share these with you. The Institute for Infrastructure and Information Assurance (IIIA) at James Madison University also provides summaries of some of their recent work.

GEORGE MASON UNIVERSITY
School of Law
CENTER for INFRASTRUCTURE PROTECTION

This month also marks the first meeting of the newly formed CIP advisory board. The meeting was held Friday, December 19th, where the board had the opportunity to meet the president of the university, Alan Merten, as well as the CIP staff. The board was briefed on an overview of CIP and the exciting new prospects our staff has been moving forward on. The board consists of a distinguished group of 16 members who provided valuable feedback and suggestions. The formation of the CIP advisory board is also a way for CIP to receive specialized guidance from board members in the different areas of infrastructure protection.

CIP has also recently welcomed the addition of Dr. KunMo Chung, a visiting distinguished professor from Korea, and Eneken Tikk, a research fellow from Estonia. Dr. Chung is an internationally known energy expert who has held posts as President of the General Conference of International Atomic Energy Agency of the United Nations, as Vice Chairman of the World Energy Council, and as Chairman of the International Nuclear Energy Academy. He will be heading CIP's work on the energy sector. Ms. Tikk is a lawyer from Estonia who is the head of the legal team for the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE). She will be lending her expertise on CIP's work in cyber conflict, including cooperative projects with the CCD COE .

We are excited about the future of CIP and look forward to continually updating you on our work and progress. We thank you for your support and wish you Happy Holidays and a great 2009!

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

Assessment of a Federal Security Program for Large Dams: Summary of a National Research Council Study

by George H. Baker, Associate Professor
Technical Director, IIIA, James Madison University

One lesson from the September 11, 2001, attacks on the World Trade Center and the Pentagon is that infrastructure built for beneficial purposes can become an instrument of mass destruction if it fails as the result of a malicious act. Dams and their related infrastructure are primarily built to control the flow of a river and mitigate flooding. The water impounded behind a dam can be used to generate power and to provide water for drinking, irrigation, commerce, industry, and recreation. However, if a dam fails, the water that would be unleashed has the energy and power to cause mass destruction downstream, killing and injuring people and destroying property, agriculture, industry, and local and regional economies.

Dam failure can occur with little warning and time for evacuation. In the worst case, where a large dam is located above a major population center, the devastation in terms of lost lives and destruction of property, power and water supply facilities, and commerce could rival or exceed that in New Orleans after the levees failed following Hurricane Katrina. Some notable examples of dam failure catastrophes are included in the table below.

Some Dam Failures and Their Consequences

Dam	Year	Location	Failure Mode	Consequences
Ka Loko Reservoir	2006	Kauai, Hawaii	Unusually heavy rain	7 killed
Val di Stava	1985	Near Trento, Italy	Poor maintenance; failure of outlet pipes	268 killed; 62 buildings and 8 bridges destroyed
Lawn Lake and Cascade dams	1982	Rocky Mountain National Park	Poor maintenance; outlet pipe erosion	3 killed; $31 million in damage (1982 dollars)
Morvi Dam	1979	India	Excessive rain; massive flooding	15,000 killed
Kelly Barnes Dam	1977	Toccoa, Georgia	Combination of factors	39 killed; property damage in surrounding area
Teton Dam	1976	Idaho	Internal erosion as dam being filled	11 killed; several towns destroyed; $300 million in damages (1976 dollars)
Banquiao and Shimantan	1975	China	Extreme rainfall beyond design capability of dam	85,000 killed

Beforet he 9/11 event, terrorists had not crashed domestic aircraft into domestic targets. At this point in history, terrorists have not exploited dams as weapons, unleashing the destructive power of the wall of water behind a dam. We must not be tempted to assume that because it has not happened in the past it will not happen in the future. Although no dam failure has yet been caused by a malicious act, the idea of causing dam failure to exploit the resulting catastrophic consequences has some notable historical precedents. Serbian forces attempted to blow up the Peruća dam in Croatia in 1993 during the Serbo-Croatian War. Hoover Dam was identified as a potential target for enemy forces during World War II. And the 1975 novel The Monkey Wrench Gang fictionalized the sabotage of Glen Canyon Dam.

The U.S. Bureau of Reclamation (USBR) is responsible for managing and operating some of this nation's largest and most critical dams, including five national critical infrastructure (NCI) facilities: the Hoover, Grand Coulee, Folsom, Shasta, and Glen Canyon dams. Reclamation's total inventory includes 249 facilities comprising

(Continued on Page 3)

1. Assessment of the Bureau of Reclamation's Security Program, National Research Council, Prepublication Copy, 19 August 2008.

Security *(Cont. from 2)*

479 dams and dikes and related facilities. The importance of the water and power supplies provided by these facilities to the quality of life in 17 western states cannot be overstated.

Recognizing the significance of dams as vehicles of mass destruction, the USBR requested the National Research Council (NRC), through the Board on Infrastructure and the Constructed Environment, to assess its security program and determine the level of preparedness to deter, respond to, and recover from malicious acts to its physical infrastructure and to the people who use and manage it. In response, the NRC appointed a multidisciplinary committee of 14 experts to perform the assessment, chaired by John T. Christian of the National Academy of Engineering. The author served as a member of this committee, which convened during the period January 2007 through September 2008.

In the course of its activities, the committee assessed security, law enforcement, and emergency management response processes, functions, andexpertise. We examined USBR's organizational structure and expertise to determine the Bureau's ability to effectively protect its physical and human infrastructure. We did not limit ourselves to USBR's present programs, but also evaluated projected changes in their security, law enforcement and emergency management operations.

The committee received briefings from the staff of Reclamation's Security, Safety, and Law Enforcement (SSLE) office and program managers from the Office of the Chief Information Officer (CIO). Groups of two or three committee members and NRC staff also visited USBR's five regions, several area offices, and a number of dam sites, including the five national critical infrastructure facilities. We interviewed USBR's area office managers, law enforcement and security personnel, and USBR contractors and operators, and we observed customs and practices of USBR staff in the field. We alsoreceived briefings and held discussions with USBR senior executives and representatives of other federal agencies involved in dam security.

The committee considered the following critical elements of a robust security program:

- Leadership and vision
- A responsive, capable security force
- Security concerns integrated into daily operations and culture at all levels
- Clear lines of authority and responsibility during normal and threat conditions
- Situational awareness aided by communication, intelligence and technology
- Defense in-depth
- A range of tools for risk assessment/mitigation
- Adequate resources – people and dollars
- Good communication internally, with the public at large, and with specific stakeholders
- Performance measurement

USBR's security challenge is multi-faceted. Chief among these is the need to balance security measures with the essential services provided by the dam infrastructure. USBR's security is complicated because their facilities are quite diverse in their design, construction, and operation. The size and characteristics of the reservoirs varies by location, season and weather conditions. Each facility possesses unique vulnerabilities which are subject to change as technology and threats evolve. Major problems can occur if a threat falls into one of the crevasses of overlapping security and law enforcement jurisdictions. Thus, USBR must carefully manage a large number of working interfaces with external government and contract organizations involved with security and law enforcement functions. These include a wide array of separate units within the Department of the Interior and other federal, state, and local agencies that vary by region and facility.

Based on its assessment, the NRC Committee determined that the USBR is better able to protect its infrastructure and its people against malicious acts through concerted efforts to expand and improve its security program since September 11th, 2001. However, the committee concluded that the security program is not yet mature, well-integrated, and appropriately supported at all levels of the organization. To date, the Bureau has focused on tactical issues that have included developing a risk

(Continued on Page 10)

Ethnographic Intelligence (ETHINT) and Cultural Intelligence (CULINT)

Employing under-utilized strategic intelligence gathering disciplines for more effective diplomatic and military planning

Written below are excerpts of an April 2008 article written by Institute for Infrastructure and Information Assurance researcher Benjamin T. Delp. This piece focuses on cultural intelligence issues pertaining to the conflicts in the Middle East. The author is currently working on an analysis of how cultural intelligence strategies have been used in recent U.S. policy to advance the Multinational Force - Iraq's objectives. The full article can be downloaded here: http://www.jmu.edu/iiia/webdocs/Reports/CulturalIntelligenceTR08-02.pdf.

Only 12 short years after the end of the Cold War, the United States began a struggle against a stateless enemy that has existed since the inception of civilization. Well-financed and educated terrorists, unified in their desire to obtain positions of power within the impoverished world, began attacking targets indiscriminately with a degree of disregard for human life not seen in at least a generation. While the terrorists appear to follow a religious agenda, one thing is certain: the terrorists who threaten to use weapons of mass destruction and kill American men, women, and children do not live in the same ideological world as U.S. citizens. The foundation of terrorism carried out in the name of Allah attempts to win over the hearts and minds of them any cultures, religions, and nation-states inhabiting the Middle East and other areas of the world. Sunni Muslims, Shi'a Muslims, Persians, Arabs, Egyptians, and other ethnic groups lead different lives compared to that of an American citizen. While there are numerous Western influences in the Middle East, and numerous Middle Eastern influences in the West, the customs, beliefs, and cultural norms of the Middle East are diverse and unlike daily practices in the U.S.

Combine a culture only a small percentage of Americans understand with a war situated in a region possessing years of ethnic tension and a major problem arises. How does the United States fight a war in Iraq, a war in Afghanistan and a political conflict against Iran, yet manage to stay out of sectarian conflicts amongst people whose divisions have been forged over thousands of years? Once the wars in Iraq and Afghanistan come to an end, how will the United States succeed in obtaining its goals of the global War on Terror? Lieutenant Colonel Fred Renzi uses Dr. Anna Simons' definition of ethnographic intelligence to answer this question:

> "What we mean by [ethnographic intelligence] is information about indigenous forms of association, local means of organization, and traditional methods of mobilization. Clans, tribes, secret societies, the hawala system, religious brotherhoods, all represent indigenous or latent forms of social organization available to our adversaries throughout the non-Western, and increasingly the Western, world" (2006, 16).

Ethnographic intelligence can then be analyzed into cultural intelligence by anthropologists, political scientists, intelligence analysts, and experts in the field to create "…an analysis of social, political, economic, and other demographic information that provides understanding of a people or nation's history, institutions, psychology, beliefs (such as religion), and behaviors." (Coles n.d., 1).

Ethnographic intelligence (EI or ETHINT) and cultural intelligence (CULINT) are not new intelligence gathering disciplines. Rather they are forms that have been overlooked during the conflicts in Iraq and Afghanistan and the larger War on Terror. High-ranking military officials, especially those teaching and studying within the prestigious U.S. war colleges, have more than made the case for increasing the amount of intelligence targeting

(Continued on Page 11)

You Can't Hit What You Can't Find
Decentralization in Infrastructure Protection

There's something to be said for a little common sense when making homeland security policy decisions. Forex ample,w henp rotectingour infrastructures, shouldn't we attempt to limit the number of available targets? If we concentrated our critical infrastructures in as few locations as possible, we could focus on stronger security procedures and better protections. With fewer available targets, we would have a better chance of predicting where terrorists might strike and what harm a natural disaster would cause us. Our nation has limited resources and a wide range of items deserving protection, so forcing a little centralization would seem to be simple common sense. If you don't have enough money to build a fence around every power plant, then maybe you need fewer power plants. Common sense seems to tell us that gathering together in a virtual "Fortress America" will make us safer.

Unfortunately, common sense is wrong. What seems like the least safe alternative on first inspection, dispersing our assets to the point where we cannot possibly track and protect them all, is actually the best choice. After all, if we can't track them, then neither can our enemies. And the farther apart our infrastructure is scattered, the less likely it is that any one natural disaster, no matter how wide-ranging, can disable a significant portion of them.

The benefits of decentralized organizations and structures have been in the news a great deal recently. Books like *The Starfish* and *The Spider*, *Wikinomics* and *The Wisdom of Crowds* have all examined different aspects of this phenomenon. Some of this is relatively intuitive. If a network, like the electrical power system, is built around one node, like the generation plant, then destroying that node brings the entire system down. It doesn't matter how many miles upon miles of wire and transformers are still in place, because those are all useless once the power plant is out of service. Conversely, if you have two, twenty, or two hundred power generation plants in operation, then you would need to lose many more than one before the system w as significantly affected. The more independent components a system has, the more difficult it is to bring that system down.

So, considering this, the conclusion most would draw is that we need to immediately start forcing a decentralization of our critical infrastructures to take advantage of these benefits. But this is the best part. We don't really need to d o anything, because this process is already in motion. Across the sectors, a decentralized architecture is developing on its own.

Coming back to electricity, it is true that no one is currently planning on building extra power plants to sit idle in case the current system is compromised. But with the advent of the Smart Grid, it is now possible to attach generation capacity at any point in the grid. The sophisticated computer programs that control the distribution network allow input of power at any point, converting the power lines from being a one-way highway to a two-way street. Power can flow in any direction, rather than just from the central plant outwards. Imagine a world where every customer can be a net power generator. This would dramatically increase the incentive to adopt renewable technologies, such as solar panels and windmills on an individual home-by-home basis. Even electrical cars could be used to move power around, by dumping their battery loads back into the electrical grid at the end of the day. Some innovative industry thinkers have even contemplated a world where a user can agree to conserve and then sell the electricity they are no longer using, thus becoming a "generator" without even acquiring any equipment.

When this system is adopted, it will not only mean benefits for the environment andlow-income customers. It will also mean benefits for infrastructure protection. When the electrical distribution grid is so spread out, it will be almost impossible to bring down. It is conceivable that the main power plant could be wiped

(Continued on Page 6)

Decentralization *(Cont. from 5)*

out without the same kind of large-scale interruption of service an event like that would cause today. This is a perfect example of the resilience that policymakers have been encouraged to adopt.

In another hi-tech field, internet service, a similar movement is taking place. Advances in wireless technology are making it possible to form ad-hoc, wide-ranging wireless networks. The technology now allows one user to plug into the internet and create a wireless "hot spot" for the surrounding area. Wireless users can create wide zones of service where the physical lines have been severed. This also allows for the maintenance of remote computer systems, so that computer control systems can be scattered rather than requiring a central processing and maintenance facility.

This interconnected network of wireless computers can be harnessed to perform complicated tasks which oncer equireda sup ercomputer. I n a process known as distributed computing, a complex processing task is broken down into a series of much smaller units and farmed out to a network of ordinary computers, to be analyzed during processor downtime. A network of ordinary computers, connected by wireless internet connections, can replicate the efforts of the most powerful and most expensive supercomputers in the world. Thus our information technology resources can also be distributed too widely to be disabled by a single event.

One such advance in the decentralization of communications technology is already too entrenched to bear notice. The infrastructure is located in a series of cell towers scattered across the landscape, rather than in a network of phone lines connected at central switching facilities. There is also the possibility that internet telephony, such as Skype, will be widely used, creating an even more decentralized communications infrastructure.

Decentralization has even found its way on to our tables with the rise of the "local food" movement. Advocates of sustainable agriculture promote more small-scale production of food on the local level. Rather than importing food across the country or across the ocean from large-scale commercial producers, communities would rely on smaller sites off arming nearby. The emphasis is on increasing organic production and personal health, but there is an infrastructure protection aspect here as well, even if unintended. The agriculture sector is dominated by large centers of food production. Contamination, accidental or intentional, at one of these facilities could shut down the transport of food all over the country. A decentralized agricultural economy would face less risk, because contamination in one locality would be much less likely to affect food in other areas.

Nothing with this much potential to improve our lives comes without a corresponding drawback. In this case, the decentralization of physical infrastructures is made possible by information technology. This technology carries its own vulnerabilities, which is why securing cyberspace, to the extent possible, is so important. Somewhat ironically, the capability to control a distant system via the internet opens it up to attacks from around the world. Attackers can now operate from anywhere there's an internet connection and they can hide their tracks with significantly more success than someone who needed to be physically present to harm the system. This is not an insurmountable obstscle, nor does it defeat the basic benefits of decentralization, but it does remind us of the perils of unabashed technological optimism.

So we see a trend. In many different sectors of the economy, technology and social attitudes are simultaneously pushing towards decentralization. Some have already noted the tendency of globalization and information technology to challenge the centuries-old trend of ever-increasing centralization and larger scales of production. A pleasant side benefit is that these trends, which are occurring for their own inexorable reasons, may make us safer by distributing our critical infrastructures outside the reach of any single large calamity. A lot can come from reconsidering one piece of common sense. ❖

Education for Infrastructure Protection

The high risk, high stakes mission of critical infrastructure protection demands a highly skilled and comprehensively trained cadre of professionals. Stakeholders and stewards of infrastructure must be able to assess risks and vulnerabilities and to develop mitigation strategies that will prevent and minimize damage. They also must be skilled in the taxing roles of leadership in crisis situations, enabling them to respond to catastrophes and restore infrastructure capabilities rapidly. This year, the Center for Infrastructure Protection has moved more decisively into the field of infrastructure protection education.

What is IP Education?

Infrastructure Protection ('IP') encompasses a range of professionals that includes engineers, security specialists, emergency responders, network/systems operators, physicists and chemists, transportation experts, policy analysts, factory managers, and much, much more. Each of these IP professions is focused on evolving its own education and training programs to continually improve the expertise and develop the necessary corps of professionals. Most of this training is targeted to the specific profession, or is delivered within the context of a specific industry sector. There has been no strong, central guidance in the development of the broader concepts of infrastructure protection. These broader IP concepts include risk analysis for homeland security purposes, information sharing across sectors and within varying levels of government, mitigation strategies to protect against cross-sector cascading effects, and global supply chain management during both natural disasters and manmade threats. Leadership in this area is badly needed — to establish standard educational and training programs for infrastructure protection, and to encourage the adoption and incorporation of these programs within the education systems of the component IP professions.

To better secure and defend our nation, a strong and continuous IP education and training system is necessary to enhance the knowledge, leadership ability, professionalism, and capabilities of IP professionals. A strategic IP education and career development system can:

(a) establish educational programs and standards for the broader concepts of infrastructure protection (those discussed above, and more); these programs are essential for (i) the development of strategic-thinking, professional IP Generalists, and (ii) incorporating the broader IP tenets into the education systems of the component IP professions (i.e., the technical specialists);
(b) effectively capture the expertise of an aging IP workforce, incorporating operational and leadership skills into the educational process;
(c) support workforce retention by providing a clear map of potential career goals, rewards, and opportunities;
(d) build a community of IP professionals with an esprit de corps that stretches across all industries and into all departments and levels of government, creating the ethos required to guide the profession; and
(e) continuously cultivate the next generation of IP leaders who push the understanding and implementation of infrastructure protection into new and unforeseen possibilities, to support the ever-changing world.

CIP Initiatives in IP Education

The Center for Infrastructure Protection ('CIP') is currently working on several initiatives in the field of IP Education. We are in the midst of discussions regarding IP Education programs with various offices within the Department of Homeland Security, the Department of Veterans Affairs, and the United States Agency for International Development. Our partners on these initiatives include George Mason's School of Law, School of Public Policy, and the Volgenau School of Information Technology and Engineering; as well as other universities and

(Continued on Page 10)

International Cyber Conflict Research

Recent cyber incidents in Estonia and Georgia serve as a powerful reminder that the United States government, the governments of other countries, and the global private sector have a long way to go in developing institutions, relationships, and doctrine to contend with malicious activity and mischief in cyber space. Notwithstanding the relative newness of the subject, a great deal of careful thought has been given to cyber conflict problems in the various fields of information technology and to the ramifications on international law and security, military operations, emergency response, telecommunications law and policy, and so on. But integrating these disparate groups and viewpoints has proved to be challenging.

For decision makers to create good policy, develop best practices, and make optimal investments, it will be necessary for experts to do more than simply address themselves to other experts in their field. The knowledge and experience of each must be put at the effective disposal of all so that we can:

(a) provide a situational assessment of the current state of affairs;
(b) identify the gaps in operations, law, and policy and determine how best to fill those gaps;
(c) share 'lessons learned' reports and 'best practices' studies among a broader community, so that our global information infrastructure may be strengthened;
(d) provide new advice and policy guidelines for government action regarding cyber incidents that do not comfortably fit within the existing legal and operational structures originally established to counteract physical-world problems of crime and warfare; and
(e) encourage the growth of collaborative relationships necessary to deal with the full spectrum of cyber conflict problems, including intra-governmental cooperation within a nation-state, cooperative relationships among nations and within existing international organizations and alliances, and mutual cooperation among private sector companies and governmental entities.

In the past year, a good working relationship has developed between the Center for Infrastructure Protection ('CIP') and the NATO Cooperative Cyber Defence Centre of Excellence ('CCD CoE') in Tallinn, Estonia. Starting in 2009, Ms. Eneken Tikk, advisor to NATO's CCD CoE, and a member of the staff of Estonia's Ministry of Defense and advisor to Estonia's departments of Justice and State, will move to the United States to become an integral member of the CIP research team on cyber conflict.

Deliverables for this project will include briefs on policy and action items, academic papers, and industry reports. Conferences and roundtables will be held to inform the project as well as share it with a wider community. This project will also incorporate its findings and deliverables as appropriate into education programs within George Mason University (e.g., public policy masters programs, courses at the law school, and classes within the school of information technology), and into study plans that will be made available to other universities and groups. CIP will encourage other schools, universities, and professional training programs, in the United States and abroad, to utilize this project's findings and deliverables. We will offer the project's documents as well as any available course texts, syllabi, and case studies. ❖

If you would like more information on CIP's International Cyber Conflict research, please contact Maeve Dion, mdion@gmu.edu.

Legal Insights

The Infrastructure Protection Mission at DHS: Past and Future

by Timothy P. Clancy, JD, Principal Research Associate for Law
and
Joseph Maltby, JD, Research Associate

Even before the creation of the Department of Homeland Security, the original concept for critical infrastructure protection was an integrated continuum of threat, vulnerability and intelligence/information sharing among and between the government and the private sector infrastructure owners and operators . This intelligence/information sharing was intended to be combined with state-of-the-art analysis of this information to enhance protection by both the government and the private sector.

Consistent with this vision, the Homeland Security Act of 2002 placed infrastructure protection in the Intelligence Analysis and Infrastructure Protection Directorate (IAIP) as part of this integrated strategy for security information sharing. Information collected and analyzed by the Office of Information Analysis (IA) would be made available to those at DHS working to protect critical infrastructures. IAIP sat alongside the Directorates of Border and Transportation Security and Emergency Preparedness and Response as one of the major mission directorates of DHS.

This arrangement has been altered substantially. As part of the Second Stage Review at DHS, the Office of Infrastructure Protection (IP) was removed from IAIP and added to a new Preparedness Directorate comprised of all of the preparedness offices within the old Emergency Preparedness and Response Directorate. IA was elevated to its own office, Intelligence and Information Analysis, and placed under a new Chief Intelligence Officer at the Undersecretary level reporting to the Secretary directly. Later, under the Post-Katrina Emergency Management Reform Act, FEMA and related functions were made an independent agency reporting directly to the Secretary of Homeland Security and the remainder of the Preparedness Directorate was renamed the National Protection and Programs Directorate, including IP.

In both cases, the Infrastructure Protection function at DHS found itself part of reorganizations brought on by high-profile controversies elsewhere. During the Second Stage Review, Intelligence Analysis was elevated to an office of its own, one of the central functions of DHS. IP was assigned to compete with a number of other "preparedness" functions within a new directorate.

These changes had more to do with concerns over the intelligence analysis or emergency response missions at DHS and less to do with IP itself. Not so much because anyone in Congress or the Executive Branch consciously decided infrastructure

(Continued on Page 12)

1. "The Department [will] build and maintain a complete, current and accurate assessment of vulnerabilities and preparedness of critical targets across critical infrastructure sectors. The Department would thus have a crucial capability that does not exist in our government today: the ability to continuously evaluate threat information against our current vulnerabilities, inform the President, issue warnings, and effect action accordingly. The National Strategy for Homeland Security, July 2002.

2. The initial proposal by President Bush for a Department of Homeland Security stated: "Under the President's proposal, the same Department that analyzes intelligence data on the potential terrorist who wants to attack the chemical plant would also be the same Department that can simultaneously alert our border security operatives, alert all of our hazardous materials facilities to ensure that they are prepared to meet this specific new threat from this specific terrorist, and alert all of the affected communities." The Proposal to Create a Department of Homeland Security June, 2002, (http://www.dhs.gov/xlibrary/assets/book.pdf, 5).

Security *(Cont. from 3)*

management program, establishing security plans for each facility, staffing a new security and law enforcement office, and developing an intelligence gathering and analysis capability. Still missing are policies and operation guidance for effective responses to security-related incidents, performance measures to support continual improvement and a method for disseminating lessons learned from incidents and exercises.

The committee recommended several strategic improvements including full support and commitment of senior executives and managers at all levels of the organization to redress problems with adequate resource availability. The Bureau has been highly successful in fostering a "culture of safety" throughout the organization. An equally strong "culture of security" is needed from headquarters to the field. The USBR's dam safety program is mature and well-integrated into the organization and serves as a good model for security program improvements. One of the highest priorities will be the development of a vision and plan to provide a path forward. The vision must explicitly link the physical assurance of USBR's facilities to its overall mission of providing water and power. ❖

The full Commission report is available at: http://www.nap.edu/catalog.php?record_id=12463.

Education *(Cont. from 7)*

Association. These programs will have different components, but of common interest are:

Academic Assessment of IP Education

We will be making an assessment of the existing IP academic courses, degrees, and research centers. Our assessment may then be combined with surveys of IP training within government and industry, to develop gap analyses and needs assessments for various agencies and government offices. This survey will also identify 'best practices' in IP education in the United States and internationally. The results of the academic assessment will also inform our various CIP curriculum development projects.

Master's Degree Curriculum in Infrastructure Protection Education

The capstone of an IP career development system would provide a master's-level IP education that cultivates senior decision-makers in the various IP component professions. The curricula will emphasize core IP competencies and will be flexible so as to adapt to the relevant component IP professions. Thus, this project will provide a core set of IP courses that could be deployed within master's-level degree programs at, for example, Schools of Business, Public Policy, Engineering, Science, Health, or Government, throughout the United States and abroad. Ultimately, our CIP non-proprietary deliverables will include recommended degree components, course outlines, suggested texts, case studies, exercises and simulations, and other teaching tools.

Training in Risk Management for Infrastructure Protection & Homeland Security

George Mason's School of Public Policy and CIP were recently awarded a grant to develop training on enterprise risk management (for homeland security) to executives in the energy sector. The training will show how risk management concepts can help provide strategic all-hazards analysis and management for critical infrastructure and key resources providers. Funded through the FEMA Competitive Training Grants Program, this project will initially be piloted in the energy sector and will be taught at various locations throughout the United States. Beyond the pilot to the energy sector, this program will be customizable for deployment to other sectors and government departments. ❖

If you would like more information on CIP's Education programs, please contact Maeve Dion, mdion@gmu.edu.

Intelligence *(Cont. from 4)*

local peoples and indigenous populations for military planning and conducting operations.

American society is filled with unwritten rules that are invisible to an outsider. An understanding of these rules allows society to function as usual. Foreign aggressors, such as terrorists, can use foreign cultures' unwritten rules against U.S. forces. Military battles against insurgents and Middle Eastern dictatorships do not pose a challenge to the U.S. military. However, winning over the hearts and minds of occupied populations is a task that cannot be accomplished through technological superiority, as articulated by Major General Robert Scales, "…the military would be much better off if it spent billions of dollars to build greater cultural awareness among military officers rather than on marginally increasing our immense technological advantages" (Coles n.d., 10). An understanding and respect for the culture of foreign populations will aid the U.S. in maximizing support against adversaries.

Additionally, Vice Admiral John Scott Redd, the former head of the National Counterterrorism Center (NCTC), articulated the need for CULINT when describing the difficulty in tracking down Osama bin Laden, "One reporter said the other day, 'Well, gee, you've got all this great overhead stuff and various surveillance things.' I said, 'Yeah. I'd trade those for about three great human sources.'" (Hosenball and Bartholet 2007, 1). Those human sources can be used for a variety of intelligence operations, from locating Osama bin Laden to creating the best plan possible to engage Iran and other militaristic states into a peaceful posture.

While portions of this essay detail ETHINT and CULINT techniques to improve current combat operations, the emphasis should be on strong collection strategies prior to engaging an enemy on hostile, non-Western terra. Certainly ETHINT and CULINT have their place in the current wars in Iraq and Afghanistan, but it would be a mistake on the part of U.S. decision-makers to overlook the value of these intelligence disciplines before military operations commence in other "hotspots."

With political unrest and regional instability running rampant throughout the world, the need for ethnographic and cultural intelligence has never been greater. While there is no one solution to bring peace and stability to the nations, religions, and ethnic groups of the world, replacing ethnocentric strategies with one that embraces the cultures of Earth for common solutions can alleviate the state of perpetual fear that has overwhelmed America. ❖

References:

Coles, John P. n.d. Cultural intelligence & joint intelligence doctrine. n.p.

Hosenball, Mark and Jeffrey Bartholet. 2007. Capital sources: The next terrorist attack. Newsweek (August 27), http://www.msnbc.msn.com/id/20466414/site/newsweek/print/1/displaymode/1098/ (accessed August 31, 2007).

Renzi, Fred. 2006. Networks: Terra incognita and the case for ethnographic intelligence. Military Review (September-October): 16-22.

Legal Insights *(Cont. from 9)*

protection was a lower priority, but the default mode is to put out the brightest and hottest fires first. The political debate in Washington regarding homeland security has, for a long time, been driven by the latest crisis. When DHS was first created, policymakers wanted to "connect the dots" to prevent another 9/11. As DHS was being reorganized, intelligence collection and analysis was still a hot-button issue and the 2005 storms made emergency response a new critical issue for debate. Thus, both the IA and FEMA functions saw their profiles raised substantially within the DHS hierarchy.

The problem is that if Infrastructure Protection is a central function of DHS as the strategic plan for the agency envisions, then placing it within an Office as part of the National Protection and Programs Directorate, among seemingly unrelated functions, seems to run contrary to that goal. Given the recent calls for DHS to place a greater emphasis on resiliency, it is prudent to ask some key questions about the infrastructure protection function at DHS: What do we want tomorrow's DHS to look like? Is the infrastructure protection function located in the right place? Is it a central mission area of DHS? If so, does its location organizationally reflect that importance? Should the Office of Infrastructure Protection be elevated to its own directorate with a broader focus on resiliency? Should it be expanded, contracted or remain the same size? How could a new infrastructure protection organization enhance resiliency?

We have had five years with a Department of Homeland Security, and protecting America's critical infrastructure remains a major strategic goal of DHS and one of the "five goals" of the Secretary. However, the office in charge of that responsibility has been shuffled aside repeatedly to make room for other more pressing matters. While endless reorganization is counterproductive, the current transition presents a good opportunity to make minimally invasive changes at DHS with potential high payoffs for security. The first Presidential transition since the founding of the Department will occur in about a month. Until now, the debate over how to focus and organize our homeland security efforts has not focused on the relative importance of infrastructure protection as a mission. Now is a good time to take stock and decide where to move forward. ❖

3. U.S. Department of Homeland Security Strategic Plan, 14.
4. James Jay Carafano, Resiliency and Public-Private Partnerships to Enhance Homeland Security, Heritage Reports, June 24, 2008, http://www.heritage.org/Research/HomelandDefense/bg2150.cfm.
5. http://www.dhs.gov/xabout/gc_1207339653379.shtm.

The Center for Infrastructure Protection 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