THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION VOLUME 7 NUMBER 5

NOVEMBER 2008
OIL & NATURAL GAS SECTOR

This month's issue of *The CIP Report* focuses on the oil and natural gas industry. Within the Energy Sector, oil and natural gas supply 65 percent of our Nation's energy and are an essential part of our everyday lives. This important source of energy fuels our cars, heats our homes, cooks our food and is vital to our economy.

GEORGE MASON UNIVERSITY
School of Law
CENTER FOR INFRASTRUCTURE PROTECTION

The first article we feature provides a brief overview of the Oil and Natural Gas (ONG) Sector. A contribution from the Vice-Chair of the ONG Sector Coordinating Council (SCC) offers information on the ONG SCC's roles and responsibilities as well as the work being done. Another key contribution discusses terrorist attacks against ONG Sector assets. The article talks about countermeasures and the possibility of future attacks and the implications. The National Petrochemical & Refiners Association (NPRA) presents an article on their role in helping to secure our Nation's petrochemical and energy infrastructures.

This month, *Legal Insights* addresses modeling and simulation (M&S). It discusses a recent workshop on M&S and how the workshop identified future research needs. Lastly, we provide an overview on the Supply Chain Security, Resilience & Sustainability Conference held October 17th and co-sponsored by CIP.

We hope you find this month's issue informative and welcome your feedback. Thank you for your continued support.

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

Brief Overview of the Oil & Natural Gas Sector

The Oil and Natural Gas (ONG) Sector is a sub-sector within the Energy Sector and comprised of production, processing, transportation, distribution, and storage of oil and natural gas. These functions rely on many interdependencies with other infrastructures, such as transportation, communications, finance, and government as well as international interdependencies. As part of the Energy Sector, ONG also contributes to the supply of energy to many other sectors and therefore creates interdependent relationships with these sectors such as Drinking Water and Water Treatment Systems, Chemical, and Information Technology.

The ONG Sector supplies over 60 percent of the energy consumed in the United States. Petroleum is primarily used in transportation, but also contributes to energy consumption within industry, residences, and commercial use. Natural gas is used residentially for heating and cooking. Power producers and industrial facilities also use natural gas for gas-powered equipment.

Infrastructure protection of the ONG Sector is a challenging task. Not only does it pose as a target for a terrorist attack, but because of its interdependencies has many vulnerabilities — from refineries and pipelines, to drilling and offshore facilities as well as secure transportation of oil and natural gas whether through ground or maritime transportation.

The Oil and Natural Gas Sector Coordinating Council (ONG SCC), formed by the oil and natural gas trade associations, represents more than 90 percent of the Sector's owners and operators. The Government Coordinating Council (GCC) is co-chaired by the U.S. Department of Homeland Security (DHS) and the U.S. Department of Energy (DOE). The ONG SCC and the Energy GCC work together assessing threats and vulnerabilities and implementing programs to better protect the Sector. The Energy GCC along with the ONG SCC and the Electricity SCC developed the Energy Sector-Specific Plan (SSP) detailing these protection efforts. ❖

SCC Members

American Gas Association
American Petroleum Institute
American Public Gas Association
Association of Oil Pipe Lines
Canadian Association of Petroleum Producers
Canadian Energy Pipeline Association
Gas Processors Association
Independent Liquid Terminals Association
International Association of Drilling Contractors
Interstate Natural Gas Association of America
Independent Petroleum Association of America
National Association of Convenience Stores
National Ocean Industries Association
National Petrochemical & Refiners Association
National Propane Gas Association
Offshore Marine Service Association
Offshore Operators Committee
Petroleum Marketers Association of America
Society of Independent Gas Marketers Association
U.S. Oil & Gas Association
Western States Petroleum Association

GCC Members

Federal Energy Regulatory Commission
National Association of Regulatory Utility Commissioners
National Association of State Energy Officials
United States Department of Agriculture
United States Department of Defense
United States Department of Energy
United States Department of Homeland Security
United States Department of Interior
United States Department of State
United States Department of Transportation
United States Environmental Protection Agency

Update – Oil & Natural Gas Sector Coordinating Council (ONG SCC)

by Ron Jorgensen, Vice-Chair, ONG SCC
Questar Pipeline Company

The Oil & Natural Gas Sector Coordinating Council (ONG SCC) continues work on an active agenda in support of the Nation's homeland security mission. The ONG SCC works closely with several Federal agencies participating on the Energy Government Coordinating Council (Energy GCC), including the Department of Energy (DOE), Department of Homeland Security (DHS), and Transportation Security Administration (TSA.) The current implementation of Chemical Facility Anti-Terrorism Standards (6 CFR Part 27) and its extensive "Chemical of Interest" list has applicability to the Oil and Natural Gas Sector, resulting in additional involvement with the Infrastructure Security Compliance Division of DHS. Good progress continues to be made on many fronts, including improvements and usage of the Homeland Security Information Network Critical Sector (HSIN-CS) as a communication platform, including use during recent major events such as Hurricanes Gustav and Ike. HSIN-CS is viewed by the ONG SCC as an essential tool for the Sector to provide real-time information sharing capability.

The ONG SCC is composed of representatives from sector owners/operators and their trade associations. The Sector is very diverse, as witnessed by the extensive list of member trade associations, requiring good communication and consensus-building. In addition to quarterly meetings and periodic classified briefings, the ONG SCC utilizes a series of sub-groups to work between meetings to advance specific issues. The SCC relies on volunteer efforts from its members, as well as some logistical Secretariat support provided through DHS and DOE. Kudos to the many dedicated sector representatives who donate their valuable time, ideas and effort to this important work under the National Infrastructure Protection Plan (NIPP.)

There are currently seven working sub-groups within the ONG SCC: Cyber/Control Systems, Chemical Facility Anti-terrorism Standards (CFATS), Emergency Management, Information Sharing (HSIN), Metrics, Pipeline, and Vulnerabilities. The Pipeline sub-group is notable in that it serves as the bridge back to TSA and the Transportation Sector,

effectively doubling as the Pipeline Sector Coordinating Council under the Transportation Systems Sector-Specific Plan (SSP). (Interestingly, oil and natural gas pipelines are involved under both the Energy and Transportation SSPs.) The Pipeline Working Group has provided input to the TSA Pipeline Security Division on updates now being made by TSA to Federal security guidance and requirements originally published for pipelines in 2002 by the Department of Transportation. TSA is currently underway on inspecting critical facilities on the 100 most critical pipeline systems as mandated by the "Implementing Recommendations of the 9/11 Commission Act of 2007." These Federal requirements are in addition to the various voluntary industry guidelines published by individual trade associations for their sub-sectors.

(Continued on Page 9)

Asymmetric Warfare Against Oil and Gas Infrastructure

by William M. (Bill) Allard*

As we approach 2009, the specter of terrorism and the impacts of terrorist attacks against oil and gas sector assets loom as ominous as ever. With national and global economies straining to breaking points, even modest acts of terrorism against oil and gas resources or facilities have far reaching impacts beyond those of the immediate, intended target.

In terms of terrorism, attacks against assets in the ONG Sector constitute the most prevalent form of asymmetric warfare that typically incurs fewer casualties. Generally speaking, economic impact is also mitigated in most cases by disconnecting or shutting down the affected resources such as pipelines before significant quantities of product are lost. The frequency of attacks against pipeline infrastructure during the past 30 years, combined with the dearth of information relative to economic and psychological/behavioral impact, makes assessing and ranking individual attacks difficult. However, there have been incidents where both loss of life and economic impact have been substantial as the result of an attack against oil and gas infrastructure.

On October 18, 1998, the National Liberation Army (ELN) bombed the Central Oil Pipeline, generating a massive fire and oil spill which inadvertently destroyed the village of Machuca, Colombia. Seventy people were killed in the resulting inferno.[1] While no specific economic impact information is available for this particular attack, according to Colombia's National Planning Department statistics, since approximately 1991, Colombian guerrillas have attacked Colombia's pipeline infrastructure more than 1,000 times, resulting in the loss of at least 2.9 billion barrels of crude and damaging ecosystems and water sources. From 1990-1995, attacks on the Cano Limon-Covenas pipeline alone resulted in a cumulative loss of nearly $1 billion; roughly seven percent of Colombia's total export revenue of $13 billion. In 2000, Colombian insurgents attacked pipelines 152 times; 170 times in 2001. [2]

In another example, on February 21, 2005, four security personnel were killed when unidentified assailants fired mortars on an oil derivatives distribution complex at the Baiji Oil Refinery, in north-central Iraq.[3] Corruption and insurgent informants working inside the Baiji refinery have compounded the problem of securing the facility and intensified the economic impact of repeated insurgent attacks against this and other facilities in Iraq. In 2005, oil production fell by 8%, averaging 1.8 million barrels per day; a million barrels fewer than before Operation Iraqi Freedom began in 2003.[4] As a result of terrorist and insurgent attacks, the Baiji refinery has shut down numerous times in the years since the war began, generally at an estimated cost of approximately $20 million per day.[5] Just in Iraq, from June 2003 through March 2008, a reported more than 460 attacks against oil and gas infrastructure prove how accessible and vulnerable these crucial energy assets are.[6]

(Continued on Page 5)

[1] Reuters, "*Colombia rebel admits oil pipeline bombing mistake*," 12 Nov 98, accessed 10 Nov 08; http://www.latinamericanstudies.org/guerrilla/mistake.htm.

[2] "*Oil and the Political Economy of Conflict in Colombia and Beyond: A Linkages Approach*," Thad Dunning and Leslie Wirpsa, University of California at Berkeley and University of Southern California, 2004, accessed 10 Nov 08; http://www.santafe.edu/files/gems/obstaclestopeace/wirpsadunning.pdf.

[3] Memorial Institute for the Prevention of Terrorism/Terrorism Knowledge Base (MIPT/TKB), "*Unknown Group attacked Utilities target*," accessed 29 Oct 07; http://www.tkb.org/Incident.jsp?incID=21895.

[4] "*Iraq: Oil Sector Faces Tough Times*," Radio Free Europe/Radio Liberty, rferl.org, 7 Feb 06, accessed 29 Oct 07; http://www.rferl.org/featuresarticle/2006/02/ddce0b02-c24d-4f9e-a262-2bf898076233.html.

[5] TheAge.com, "*Insurgents shut Iraq's largest oil refinery*," 31 Dec 05, accessed 10 Nov 08; http://www.theage.com.au/news/world/insurgents-shut-iraqs-largest-oil-refinery/2005/12/30/1135915690925.html.

[6] IAGS ENERGY SECURITY, "*IRAQ PIPELINE WATCH: Attacks on Iraqi pipelines, oil installations, and oil personnel*:" 27 Mar 08, accessed 5 Nov 08; http://www.iags.org/iraqpipelinewatch.htm.

Asymmetric Warfare *(Cont. from 4)*

On February 24, 2006, Al-Qaida suicide bombers attacked the Abqaiq oil refinery near Buqayq in eastern Saudi Arabia with two Vehicle-borne Improvised Explosive Devices (VBIEDs), though they were unsuccessful in gaining access to the complex. Security guards fired on the vehicles and the devices detonated at the outer perimeter, killing two terrorists. Two security guards were also killed in the explosions.[7] The Abqaiq facility is the largest oil refinery in Saudi Arabia, processing 5-7 million barrels of oil per day or roughly two-thirds of the country's total oil output. Immediately following the attack, futures on light sweet crude oil for April 2006 delivery jumped from $2.16 to $62.70 per barrel on the New York Mercantile Exchange though no damage to the Abqaiq refining processes or equipment occurred.[8] Despite the enormous footprint the petroleum industry has in Saudi Arabia and though terrorist attacks against oil-industry workers have occurred periodically over the years, the Abqaiq facility incident was one of the most brazen terrorist attacks against refinery operations in the Kingdom.[9]

As recently as October 2008, in North America, authorities of the Royal Canadian Mounted Police (RCMP) continue investigating the attacks of October 12 and 17, 2008 on EnCana Corp. natural gas assets in British Columbia. Both attacks appear to be related, according to RCMP authorities, who have made no arrests in the incident.[10]

Countermeasures

In parts of the world where the threat of hostilities is ever present, such as Iraq, Colombia, parts of the African Continent, and even international waters such as the Indian Ocean, preventing and countering attacks against oil and gas assets remain daunting challenges. Use of airborne surveillance to monitor pipelines, applying additional security personnel to protect critical land-based nodes, and escorting vessels through hostile water-routes are costly but proven effective deterrents that force adversaries to turn to other attack methods such as the use of stand-off weapons which may be less effective, yet offer greater security for the attacker.[11]

The Saudi Arabian government has created the Petroleum Facilities Force to guard the country's massive oil and gas resources and is in the process of posting upwards of 35,000 troops and security forces along pipelines, oil fields, and processing plants.[12] In critical sea lanes such as the Strait of Hormuz, the Strait of Malacca, and the Red Sea, protecting highly vulnerable vessels from attack involves multinational commitments to the safety of the crews and the security of the product they carry. In 1987, during the final throes of the Iran-Iraq War, the United States launched Operation Earnest Will; the reflagging of Kuwaiti tankers in efforts to end the siege against the region's oil and gas assets from attacks from Iran. By early 1988, naval forces from at least 10 western countries were in service in the Persian Gulf, repelling aerial attacks, removing sea mines, and protecting tankers through the volatile region.[13]

(Continued on Page 10)

---

[7] "*Communiqué from Al-Qaida's Committee in the Arabian Peninsula (Saudi Arabia)*," 24 Feb 06, accessed 10 Nov 08; http://www.globalterroralert.com/pdf/0206/saudi0206.pdf.

[8] "*Guards Foil Attack on Saudi Oil Refinery*," Associated Press on Fox News.com, 24 Feb 06, accessed 10 Nov 08; http://www.foxnews.com/story/0,2933,185910,00.html.

[9] "*Two attackers were on Saudi's most-wanted list, Men died in Friday's attack on oil processing complex*," Associated Press on MSNBC, 26 Feb 06, accessed 10 Nov 08; http://www.msnbc.msn.com/id/11538965/.

[10] Ottawacitizen.com, "Second bomb attack hits northern B.C. natural gas pipeline," 17 Oct 08, accessed 5 Nov 08; http://www.canada.com/ottawacitizen/news/story.html?id=7536c750-8a4a-4d23-a069-b92512955396.

[11] Oil and Gas Industry Terrorism Monitor, "A Synopsis of the Terrorist Threat Facing the O&G Industry," 2007, accessed 5 Nov 08; http://www.ogi-tm.com/ogi_threats_st.php.

[12] Dallas News.com; "Saudi Arabia works to protect oil fields from terrorism," 5 Dec 07, accessed 10 Nov 08; http://www.dallasnews.com/sharedcontent/dws/bus/stories/DN-OilSecurity_05bus.State.Edition1.1c0e94d.html.

[13] GlobalSecurity.org, "Operation Earnest Will," 27 Apr 05, accessed 10 Nov 08; http://www.globalsecurity.org/military/ops/earnest_will.htm.

Petrochemical & Refining Facilities Working on DHS Site Security

by Jeff Gunnulfsen, Director of Security and Risk Management, NPRA

The National Petrochemical & Refiners Association (NPRA) is a national trade association whose nearly 500 members include virtually all refiners and petrochemical manufacturers in the United States. Our members supply consumers with a wide variety of products and services that are used daily in homes and businesses. These products include gasoline, diesel fuel, home-heating oil, jet fuel, asphalt products, and the chemicals that serve as "building blocks" in making plastics, clothing, medicine, and computers.

NPRA members are absolutely committed to securing our facilities from the potential threat of terrorism. We are proud of our successes in working with local, state, and federal agencies and departments to maintain, secure, and strengthen the critical petrochemical and energy infrastructure of our nation.

Refining and petrochemical businesses have always placed great emphasis on facility security. NPRA's members have been actively implementing security measures long before the Chemical Facility Anti-Terrorism Standards (CFATS) were developed, to ensure protection against such potential threats as trespassers, eco-terrorists, insurgencies, natural disasters, and other contingencies.

NPRA has been engaged with DHS's Critical Infrastructure Protection Office since its inception. The following are just a few of the DHS site security projects that NPRA and its members have participated in:

- Development of Security Vulnerability Assessment (SVA) Methodology for the Petroleum and Petrochemical Industries (October 2004)
- DHS Industry Security exercises
- Risk Analysis and Management for Critical Asset Protection (RAMCAP) exercises (2004)
- Creation of Facility Security Officer Training Course (2005)
- Chemical and Oil and Natural Gas Sector Coordinating Councils as members
- Hurricane Preparedness and Reliability work with DHS
- NPRA Security Conference

Additionally, many NPRA member facilities are subject to the Maritime Transportation and Security Act (MTSA). NPRA's members worked hard to comply with MTSA prior to CFATS and are currently working towards implementation of the Transportation Worker Identification Credential (TWIC) program. NPRA members and their facilities may be affected by either CFATS or MTSA — and, in many instances, by both. Currently, many companies are completing their Security Vulnerability Assessments (SVAs) and beginning to review the DHS Risk-Based Performance Standards (RBPS) to help them prepare their Site Security Plans (SSPs). NPRA comprises of member companies in both the Chemical and Energy Sectors, and a terrorist attack on any such facility has the potential for severe consequences locally, regionally, and nationwide. The operators of those facilities are thus working hard to implement new security regulations to enhance and strengthen the substantial security measures already in place.

The incoming 111th Congress is expected to take up chemical site security legislation, as the current program sunsets in October 2009. NPRA supports legislation that would allow the current regulatory program to continue as is. The initial requirements of the original CFATS statute are only now beginning to be fully implemented. NPRA does not support legislation that would mandate Inherently Safer Technology (IST). Mandating IST will create needless burdens and possibly threaten consumer choice. Because safety is the top priority of domestic chemical businesses, facility operators already utilize the safest and most innovative security measures available. ❖

Legal Insights

Future Research Needs in Modeling and Simulation for Homeland Security Report from a DHS Science and Technology Workshop

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

Last month I participated in a DHS-sponsored workshop on future needs in modeling and simulation (M&S). The Department of Homeland Security, Science and Technology Directorate (DHS-S&T) convened the workshop entitled, "Future Directions in Critical Infrastructure Modeling and Simulation" held at the Virginia Modeling, Simulation and Analysis Center in Suffolk, Virginia.

The objective of the workshop was to provide a forum for researchers and practitioners dealing with critical infrastructure M&S with a focus on multi-events, multi-threats and cascading effects. Workshop participants sought to assess the current state-of-the-art in M&S, identify challenges, and develop strategies for addressing these challenges. The results of the workshop should help DHS-S&T formulate near and long-term investment decisions as well as research strategy, plans, and objectives for M&S of the Nation's critical infrastructure and key resources (CI/KR).

The workshop was invitation-only and featured top experts on M&S from academia, industry, and government. Due to the complexity and interdependent nature of the Nation's CI/KR, sophisticated M&S capabilities have been seen as vital for DHS to fulfill its CI/KR mission. Congress in the Homeland Security Act of 2002 called for the transfer of the National Infrastructure Simulation and Analysis Center (NISAC) at Sandia and Los Alamos National Laboratories, formerly part of DOE.

Also participating, from George Mason University, was Dr. Kevin McCabe, Director of the Center for the Study of Neuroeconomics (CSN) and Dr. Jim Kadtke, Fellow of the George Mason University Center for Infrastructure Protection (CIP). Dr. McCabe presented findings from the CSN on the modeling and simulation of complex economic decision-making environments such as stock markets as well as recent findings on human cognitive behavior in trust environments. This research is now being applied to the social and economic activities found in the online virtual world SecondLife™.

Dr. McCabe briefed attendees on a tool being built in SecondLife™ that uses agent-based modeling to populate a dedicated island with avatars equipped with artificial intelligence. The experimental island with its economic systems and critical infrastructures will be subjected to all kinds of hazards and disaster scenarios, and the following responses and events simulate the real world. This will be used as a training device and a model to assist decision-makers in crisis situations. The simulations will produce "best practice" rules for creating the next generation of virtual operations or crisis management centers and for training programs.

In addition, Dr. Kadtke chaired a breakout group that discussed which models are best suited for certain applications in critical infrastructure protection. The breakout group reviewed three areas: 1) the types of modeling, simulation, and computational analysis methods currently available, 2) the classes of DHS problems and requirements they are most suited for, and 3) the technical maturity of the capabilities. The group then constructed a matrix of M&S capabilities versus DHS CI/KR challenge areas.

Another breakout session analyzed the research gaps and needs to guide future planning for DHS-S&T. One gap cited by workshop attendees was that models for complex human behaviors were often lacking in current CI/KR models. Several people observed

(Continued on Page 11)

Experts Advocate More Effective Public-Private Risk Management Models at Supply Chain Security, Resilience & Sustainability Conference

Dr. James Carafano, of the Heritage Foundation, and fellow experts advocated increasing the effectiveness of public-private risk management models at the October 17th Annual Supply Chain Security, Resilience and Sustainability Conference, co-sponsored by six Washington, DC area organizations and hosted by George Mason University's Center for Infrastructure Protection (CIP).

"Define what is reasonable to achieve between the private and public sector through clear processes and performance measures. Create transparency and the means to measure performance. Provide legal protections to encourage information sharing and be tailored to the unique characteristics of each sector," said Dr. Carafano, an expert in Homeland Security who has testified several times in Congressional hearings and was the plenary session speaker at the conference.

"Our conference brought an exciting group of representatives from government and the commercial sector, who share responsibility to ensure that our economy and our role in the global economy understand the importance of optimizing the efficiency of supply chain operations while minimizing its vulnerability to disruption," said Dr. Jane Feitler from the National Capital Area Roundtable of the Council of Supply Chain Management professionals. Dr. Feitler's organization was a co-sponsor along with George Mason University's CIP, the Supply Chain Council, the American Society of Transportation and Logistics, DC Metro APICS, and the Washington, DC Thunderbird Alumni Association.

The audience of supply chain professionals was provided with specific tool sets to better manage risk, including the Supply Chain Council's SCOR 9.0 model. Taylor Wilkerson, a Research Fellow at LMI, who presented on the SCOR model said, "Risk mitigation is now a component of Total Supply Chain Management Cost and provides the total of these costs across all the processes."

Supply Chain sustainability was a focus of the Triple Bottom Line and another presentation at the conference offered by Karen Felstein, a consultant with Booz Allen Hamilton, who stated, "People, planet and profit work in tandem; no one part can make measurable impact without the other." A panel of experts from the government and from George Mason University discussed the trade-offs and challenges to balance how far government should go to incentivize or regulate supply chain resilience. Additional sessions focused on enterprise risk identification, safeguarding supply chains from geopolitical risks, and tools for preparedness and resilience in supply chains.

To view some of the presentations from the conference, please visit http://cipp.gmu.edu/research/SupplyChainConferencePresenters.php or for further information contact Irvin Varkonyi at ivarkonyi@scopedu.com, (703) 863-9686.

ONG SCC *(Cont. from 3)*

Each of the working sub-groups within the ONG SCC has a chairperson, volunteers from within the SCC, as well as outside experts where needed. In many instances, the working sub-group coordinates closely with one of the partner agencies. For example, the Metrics group continues to work closely with DOE (the Sector-Specific Agency for Energy) on the development of streamlined metrics that will help demonstrate the good progress being made across the diversity of the Sector. Currently, the Metrics group is following up on a workshop held in Houston on August 19, 2008 that suggested various new physical and cyber/SCADA metrics.

The ONG SCC is also an active participant in the Partnership for Critical Infrastructure Security (PCIS.) The ONG SCC leadership (Chair/Vice-Chair) represents the Sector with PCIS. PCIS continues to serve as an effective advocate for the value of the public/private partnership across all 18 critical infrastructure and key resources, including Energy. PCIS continues to promote a number of initiatives, including greater private sector involvement in National Level Exercises.

One of the greatest challenges facing the ONG SCC is scope-creep. It is inherent with the multi-agency structure created under the NIPP, combined with new legislative and regulatory mandates, that there will be some degree of fragmentation — essentially, a plethora of independent initiatives. Multiplied by all the additional activities at the regional, state and local levels, this becomes a challenge for the Sector. One of the current goals for the ONG SCC at the Federal level is to encourage greater coordination and prioritization of these multiple Federal initiatives. Work is now beginning on a centralized planning calendar that would provide each of the Energy GCC partners a tool to help coordinate the various activities, set priorities, and avoid unnecessary conflicts (e.g. overlapping meetings/deadlines.) More progress on this priority is needed in 2009 as there is an opportunity for stronger coordination between agencies, as well as some further rationalization of this complex (multiple agency) oversight structure. The ONG SCC applauds all of the good efforts made to-date by DOE, DHS, TSA and the other GCC agencies in support of our mutual objectives.

Overall, there has been very good work and progress made in the Sector as a result of the efforts made on both the public and private sides of the partnership, enabled in large measure by CIPAC (Critical Infrastructure Partnership Advisory Council), and guided by a risk-based framework under the NIPP. While the initial shock and horror of 9/11 may be several years behind us, it has left a lasting impression on the men and women of the Oil and Natural Gas Sector. The challenges of securing critical facilities, preparing for emergencies, and promoting sector resiliency remain paramount. The ONG SCC looks forward to continuing all of these efforts under the NIPP in consultation with DOE, DHS, TSA and all of the Energy GCC agencies.

Looking forward, the transition to working with a new Administration will provide a tremendous opportunity to identify and reinforce what has been successful, examine new ideas and vision, and jointly pursue a pathway forward that best serves our national interests on the energy front. Many good concepts have been embraced to-date, including public/private collaboration and a risk-based approach. The ONG SCC is poised and ready to continue its active support for this critical mission. ❖

Asymmetric Warfare *(Cont. from 5)*

Future of Attacks and Possible Implications

Though the numbers of insurgent and terrorist attacks in Iraq in 2008 are thankfully on the decline with October 2008 numbers of violent deaths falling to its lowest since the start of the war in 2003, insurgent and terrorist attacks still occur routinely in the region.[14] Compounding the difficulties encountered with stabilizing Iraq and the Iraqi oil market are the controversies surrounding commercial petroleum agreements with the fledgling Iraqi government. It's very unlikely that any negotiated deal on the future of Iraq's oil and gas resources will satisfy all political parties and these dissatisfactions may result in persistent, violent interruptions of oil and gas refining and distribution.

Yet despite the drop in demand of petroleum products in recent months, the need for fossil fuels can be expected to continue and indeed grow with recovering economies at least until viable alternative fuel solutions become more pragmatic and cost-effective. According to the Energy Information Administration of the U.S. Department of Energy, global demand for oil is expected to increase by 54% in the first 25 years of the 21st century, meaning oil producing nations will need to increase their production by an additional 44 million barrels per day by the year 2025.[15] If these projections are accurate, petroleum and derivative goods will become increasingly valuable and costly to protect. Tensions over ownership of these precious resources will manifest itself quickly and violently. Even today, the governments of Myanmar and Bangladesh are rapidly closing the gap between frustration and conflict over sovereign ownership of the rich hydrocarbon deposits in the Bay of Bengal.[16]

Among the variables that can influence the future security of the oil and gas industry, three constants can be relied upon; the fragile nature of geo-political relationships that hinge upon robust petroleum-based economies; the challenges faced by countering and mitigating random political-ideological forces that can and oftentimes inflict costly damage; and that oil and gas infrastructure will remain expensive but necessary targets to protect for the foreseeable future. ❖

* William M. (Bill) Allard is a Senior Analyst for CENTRA Technology, Inc., currently providing intelligence analytical support to U.S. Government client agencies. Mr. Allard is retired from the U.S. Marine Corps and has been a member of the National Intelligence Community for more than 27 years. As a former Sr. Intelligence Analyst and Acting Division Chief of the Critical Infrastructure Protection Division at the Department of Defense's Counterintelligence Field Activity, Mr. Allard authored and supervised production of more than 100 issues of CIFA's "CIP Weekly Highlights," and numerous other CIP-related studies and multi-discipline threat assessments for DoD.

[14] Daily Nation, (Kenya), "13 Killed as blasts rock Baghdad," 5 Nov 08, accessed 5 Nov 08; http://www.nation.co.ke/News/world/-/1068/487260/-/ryu19g/-/.

[15] CBC News Online: "Supply and demand: World oil markets under pressure," 28 Apr 05, accessed 10 Nov 08; http://www.cbc.ca/news/background/oil/supply_demand.html.

[16] Voice of America (VOA.com); "Bangladesh, Burma Dispute Oil Exploration in Bay of Bengal," 4 Nov 08, accessed 5 Nov 08; http://voanews.com/english/2008-11-04-voa8.cfm.

Legal Insights *(Cont. from 7)*

that M&S is not really a tools problem — there were plenty of excellent sophisticated and useful M&S tools spurred by Moore's law and exponentially higher computer speeds. However, integration of social, economic, and behavioral models into existing capabilities was needed for better understanding of interdependencies and cascading effects across infrastructures.

Another gap was that few of the non-DHS attendees seemed familiar with DHS CI/KR doctrine enshrined in the National Infrastructure Protection Plan (NIPP) and other documents. Since NIPP represents a comprehensive risk model that should guide key CI/KR stakeholders — including state, local, and tribal governments — it is necessary that any DHS M&S research plan better incorporate NIPP principles. Also, further NIPP development, refinement, and deployment by DHS Office of Infrastructure Protection should utilize M&S capabilities being developed by the S&T Directorate.

Over the next few years it will be vital for all relevant stakeholders to begin utilizing the NIPP risk model more fully into their CI/KR protection plans. This is especially true for state, local, and tribal governments in their role as first responders and primary providers of domestic security. Many M&S tools are currently oriented toward national needs and priorities with less priority given to regional, state, and local needs. Greater attention must be given to M&S capabilities that incorporate the NIPP and can be used more widely by state and local officials. Given that powerful M&S capabilities are already used extensively at the local level in municipal planning as well as environmental and resource management, it would be prudent to analyze these fields for M&S best practices in homeland security. ❖

The CIP Program 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 CIP Program is funded by a grant from the National Institute of Standards and Technology (NIST).

The CIP Report is published by Zeichner Risk Analytics, LLC (ZRA) on behalf of the CIP Program. ZRA is the leading provider of risk and security governance knowledge for senior business and government professionals. ZRA's vision is to be a consistent and reliable source of strategic and operational intelligence to support core business processes, functions, and assurance goals.

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