THE CIP REPORT

CRITICAL INFRASTRUCTURE PROTECTION PROGRAM VOLUME 5 NUMBER 10

APRIL 2007

CIP ACADEMIC RESEARCH

In this month's issue of *The CIP Report*, we highlight three examples of ongoing academic research directly impacting not only the field of critical infrastructure protection, but national security writ large. These contributions, provided by researchers at James Madison University and George Mason University, and a recent graduate of American University, look at very distinct areas of interest: the first looks at high altitude nuclear weapon detonation and the subsequent impact of an electromagnetic pulse (EMP) on infrastructures; the second examines the ongoing academic debate on open publication of scientific journals and the potential that such research could be used to create a so-called 'poor man's weapon of mass destruction'; and finally, the third article is a comparative analysis of the development of homeland security partnerships. While these three articles are very diverse examples of ongoing critical infrastructure and national security related research, they serve as a sampling to show the breadth and depth of academic resources devoted to these issues.

In addition to these contributions, we also highlight the recently passed 9/11 legislation, 'Improving America's Security Act,' with details of CIP related language, as well as the recent DHS leadership appointments and resignations. Finally, we include a Legal Insights column focusing on the threats to the Commercial Facilities sector, specifically shopping malls, and an invitation to a symposium on Internet Governance and Internet Security, to be held on May 17, 2007 at the Swiss Embassy.

On a sadder note, the CIP Program has been privileged to work with a number of Virginia Tech researchers, and during this difficult time, our thoughts are with our colleagues and the entire Virginia Tech community. As always, we hope you enjoy this issue and appreciate your continued support of the CIP Program.

John A. McCarthy
Director, CIP Program
George Mason University, School of Law

EMP – A National-Scale Threat to the U.S. Infrastructure

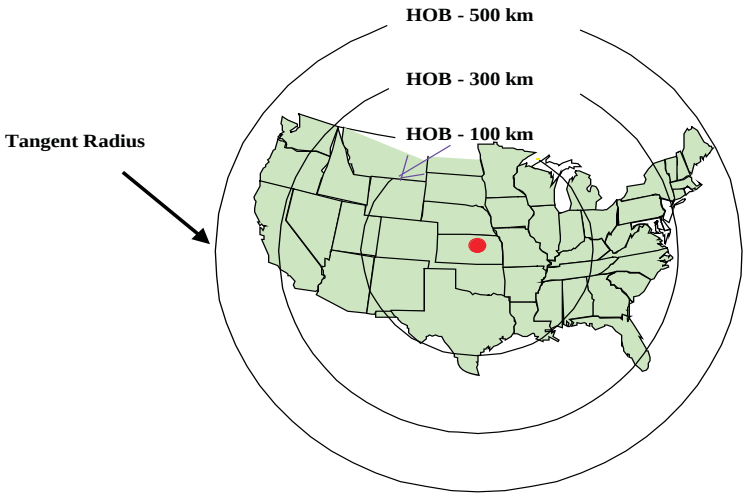
George H. Baker, Associate Director
Institute for Infrastructure and Information Assurance
James Madison University

Since the nuclear weapon atmospheric test days of the 1950s, it has been known that a single nuclear weapon detonated at altitudes from about 30-500 kilometers generates a strong electromagnetic pulse (EMP) that can disrupt electronic systems on the ground at large distances from the burst. During the Cold War, the effects of high altitude nuclear detonations were considered by many to be ephemeral, second order effects in comparison to direct blast/thermal/radiation effects from near-surface bursts in the context of mutually-assured-destruction (or MAD) scenarios. However, as infrastructure objectives have gained prominence in military operations, the likelihood of high altitude nuclear scenarios have gained wider acceptance among strategic planners. When viewed in the context of infrastructure debilitation, high altitude nuclear attacks begin to make sense as a primary tactic to deny or delay an adversary's ability to respond. The use of nuclear weapons at high altitudes could prove decisive in future conflicts.

Because a national-scale disruption may accrue from the detonation of a single weapon, EMP is arguably the most serious threat to U.S. infrastructure. The EMP induces large voltages and currents in wires and antennae connected to electronic systems that may upset operation or damage circuit components. Integrated circuits used in computers, infrastructure controls, and communication systems are particularly susceptible to these effects. Long line networks such as the electric power grid and telecommunications systems receive and propagate the largest EMP currents, making them most likely to fail. The military has taken steps to protect its most critical systems. The civilian economy has not.

In 2002, recognizing our crucial dependence on advanced electronic systems, Congress established a nine-member panel headed by Reagan administration science adviser, William Graham, to examine the threat from such an explosion to critical infrastructure. Representative Roscoe Bartlett (R-Md.) wrote the legislation to create the Commission. The Commission issued its report to Congress in 2004. The EMP Commission hearing was eclipsed by the 911 Commission hearing which was held on the same day. The report represents the unanimous views of the Commission members.

The Commission's unclassified executive summary recognizes EMP as one of a very small number of threats that can hold the entire nation at risk in terms of significant damage to critical infrastructures and the ability of the United States to project influence and military power. The Commission explains
(Continued on Page 3)



Single High Altitude Detonation EMP Ground Coverage for 3 Heights of Burst (HOB)

"The effect is asymmetric, both in terms of the continental-scale effects from a single weapon, and that potential protagonists do not depend upon electronics to the extent that we do."

EMP *(Continued from Page 2)*
that our vulnerability is increasing daily because of our growing dependence upon electronics. The effect is asymmetric, both in terms of the continental-scale effects from a single weapon, and that potential protagonists do not depend upon electronics to the extent that we do. The report identifies several potential adversaries that have or can acquire an EMP attack capability, including China, Russia, North Korea, Iran and non-state malefactors. Achieving an attack capability is facilitated by the fact that there is no need to smuggle a weapon across the border (an offshore detonation will expose large, adjacent land areas) and no need for missile sophistication or accuracy. Short-range Scud missiles, readily available on the international arms market, are sufficient to get a nuclear weapon to the required altitude. The Commission expressed concern that the present vulnerabilities of our critical infrastructures both invite and reward attack if not corrected. The Commission is convinced that correction is feasible and well within the Nation's means.

The Commission provides guidance for reducing long-term consequences below catastrophic levels. This will require a coordinated and focused effort between private industry and the public sector. The Commission projects the cost for such improved security in the next three to five years to be modest when compared to the war on terror and the value of the national infrastructures at risk. Preparations will involve a balance of prevention, protection, planning, and preparations for recovery. A number of these actions will also reduce vulnerabilities to other serious threats to our infrastructures.

It will be important to identify and protect key vulnerabilities in the most critical infrastructure systems. Recognizing that it is not possible to protect everything, planning is needed to recover essential services to eliminate adversaries' prospects to achieve large-scale, long-term infrastructure outages. The Commission believes that adequate preparation could be achieved within three to five years, given a dedicated commitment by the federal government and an affordable investment of resources.

Because of the national security implications of EMP, the Commission recommends that the federal government shoulder the responsibility of managing the most serious infrastructure vulnerabilities per Homeland Security Presidential Directives 7 and 8. These Directives give DHS the authority it needs to deal with civilian consequences of an EMP attack. The Commission laid out the following strategy to address the EMP threat:

- Pursuit of intelligence, interdiction, and deterrence to discourage an EMP attack against the U.S. and its interests.
- Protecting critical components of the infrastructure, with particular emphasis on those that, if damaged, would require long periods of time to repair or replace.
- Maintaining the capability to monitor and evaluate the condition of critical infrastructures.
- Recognizing an EMP attack and understanding how its effects differ from other forms of infrastructure disruption and damage.
- Planning to carry out a systematic recovery of critical infrastructures.
- Training, evaluating, red-teaming, and periodically reporting to Congress.
- Defining the Federal Government's responsibility and authority to act.
- Recognizing the opportunities for shared benefits.
- Conducting research to better understand infrastructure system effects and developing cost-effective solutions to manage these effects.

Details of this strategy are included in the Executive Summary, available at the following website: http://empcreport.ida.org.

Because of the material implications of the initial Commission findings and recommendations, the current Congress has rechartered the group to assist in planning and implementation. ❖

Senior DHS Leadership Appointments

Secretary of Homeland Security, Michael Chertoff, recently announced a number of senior leadership appointments in the Department.

National Protection and Programs Directorate (NPPD)

Robert D. Jamison will serve as the Deputy Under Secretary for the National Protection and Programs Directorate. Robert will help lead national efforts to protect critical infrastructure and prevent attacks on it and improve the resiliency of essential cyber-security and communications capabilities.

Robert A. Mocny will serve as the director of the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program. Robert has been the Deputy Director of US-VISIT, and has recently served as the program's Acting Director. He will continue to oversee the important work of US-VISIT, balancing the security of citizens and visitors through biometric authentication, while facilitating legitimate trade and travel.

Federal Emergency Management Agency (FEMA)

Christopher T. Geldart will serve as the director of the Office of National Capitol Region Coordination (ONCRC) within FEMA where he will oversee and coordinate federal programs and domestic preparedness initiatives for state, local and regional authorities in the National Capital Region.

Dennis R. Schrader has been nominated by President Bush to be the Deputy Administrator for National Preparedness, Federal Emergency Management Agency (FEMA). Mr. Schrader is thoroughly familiar with the needs of state and local emergency management, having been Maryland's first Homeland Security Advisor and responsible for partnering with the National Capital Region jurisdictions to develop homeland security programs in the area.

Policy Directorate

Tom Lockwood has been appointed as Senior Advisor for Credentialing Interoperability with the Department of Homeland Security's Screening Coordination Office. In his new capacity, Tom will build on his pioneering success in developing common interoperable credentials for public and private sector first responders by working on key secretarial screening initiatives including fostering interoperability of credentialing systems for federal, state, and local governments. ❖

Statement by Homeland Security Secretary Michael Chertoff on the Resignation of Under Secretary George Foresman

Today, I accepted the resignation of George Foresman as Under Secretary at the Department of Homeland Security, effective in the coming weeks. George has given me and the entire senior leadership team wise counsel in addressing complex homeland security challenges under trying conditions. George is an exceptional professional who has shown a steadfast commitment to the ideals of leadership by example. Prior to coming to the department, George spent more than 20 years in local and state government in Virginia and is respected around the country for his bi-partisanship and expertise. Through his tireless dedication, George helped sharpen the federal government's focus in the areas of infrastructure protection, including the security of chemical facilities, national information technology and telecommunications systems, and he has been instrumental in leading refinements to our grants processes, approaches to risk management, use of biometrics, and communications interoperability. I am grateful for George's service to the American public and his lasting contributions to the security of our homeland. I regret seeing him leave, and look forward to our continued friendship.

Legal Insights

Shopping Malls – Possible Terrorist Target?

Colleen Hardy
Senior Research Associate , CIP Program

In the December 2006 issue of *The CIP Report*, I discussed a case where patrons were searched and patted down before entering an NFL Stadium. National security concerns have raised awareness and measures at an array of commercial facilities including arenas, hotels and stadiums. Shopping malls have also increased efforts and attention to security details and plans. The Department of Homeland Security categorizes shopping malls as soft targets. National security experts have debated whether shopping malls are a potential terrorist target, and if they are, what actions should be taken to prevent such attacks. An important aspect that experts examined is how much security shoppers will tolerate at shopping centers. For example, will shoppers tolerate pat downs or metal detectors at mall entrances similar to those conducted at stadiums? As one commentator stated, "Their challenge is in finding the balance of security measures that provide customers with confidence in their safety while allowing them to shop in a friendly, welcoming environment."

According to an International Council of Shopping Centers (ICSC) report released in March 2005, 87 percent of shoppers felt that enclosed malls were safe and a majority of shoppers stated they do not alter their shopping habits when the government elevates the national threat advisory. Despite the high number of shoppers who are not worried about terrorist threats to shopping centers, several shopping malls across the country have increased security efforts to protect their patrons and shopping centers from a terrorist threat.

For example, some shopping malls have initiated emergency evacuation drills and enhanced their surveillance equipment. Additionally, some shopping malls have installed bollards at mall entrances to prevent and deter terrorists from driving into the mall. Other shopping centers have altered their security staffing requirements, such as conducting background checks on security guards and also placing police officers (in addition to civilian guards) inside the shopping malls. Furthermore, more emphasis has been placed on training observation skills for security personnel and increased presence.

One security expert stated that alarm systems protecting against biological and chemical attacks are likely to be implemented in malls within the next few years. Other experts ascertain that training security guards is the most effective element to prevent an attack, versus utilizing expensive security systems.

The International Council of Shopping Centers has taken an active role to help security personnel and mall owners understand and address potential threats to shopping malls. The ICSC also partnered with the Homeland Security Institute at George Washington University to create a training program for shopping mall security personnel. According to one report, the 14 hour training program is the first standardized training course established specifically for the nation's estimated 20,000 mall security guards. The program was developed based on DHS' terrorism response guidelines and consists of 10 DVD courses including an introduction; the National Incident Management System and National Response Plan; the history and threat of terrorism; the North American Emergency Response Guide; chemical terrorism; biological agents; radiological and nuclear terrorism; explosives; behavioral awareness; and suicidal terrorism. The goal of the ICSC and GW training program is to train guards to be more aware of the effects of a terrorist attack and to teach them to identify potential attackers. For example, the program instructs security personnel to look for possible suicide bombers by looking for individuals who are unusually dressed, such as an individual wearing a heavy coat in the middle of the summer. In February 2007, Paul Maniscalco, a senior research scien-

(Continued on Page 6)

Legal Insights *(Continued from Page 5)*

tist at GW who helped create the program, reported that the program completed testing at a few shopping malls and is scheduled to be implemented over the next month.

In an ICSC survey conducted in 2005, shoppers stated "they would be willing to put up with more-stringent security efforts, such as metal detectors, but only if DHS were to raise the national threat level." However, some security experts state the best weapon is people's eyes and ears emphasizing the more eyes you have looking for a suspect, the more likely you will find him. In the past few years, there have been a few threats concerning mall safety.

In 2005, the FBI arrested a man for his alleged plans to blow up a shopping center in Columbus, Ohio. It is alleged that he traveled to Ethiopia to receive terrorist training. He is currently awaiting his trial.

In December 2006, federal agents arrested Derrick Shareef "on charges of planning to detonate hand grenades at an Illinois shopping center on December 22nd as part of his plan to commit 'violent jihad' against civilians." Shareef was arrested when he met with an undercover agent to trade a set of stereo speakers for four grenades and a handgun. The special agent in charge of his case stated Shareef chose December 22 because it was the Friday before Christmas and therefore the mall would be exceedingly crowded and he would have a greater chance at achieving a larger number of casualties. The FBI worked with an informant to apprehend Shareef. Prior to his arrest and under FBI surveillance, Shareef and the informant walked around the targeted shopping center discussing the layout and ideal locations to detonate the grenades. Shareef was charged with one count of attempting to damage or destroy a building by fire or explosion and one count of attempting to use a weapon of mass destruction. He was indicted in January 2007 and is awaiting trial.

"One security expert stated that alarm systems protecting against biological and chemical attacks are likely to be implemented in malls within the next few years. Other experts ascertain that training security guards is the most effective element to prevent an attack, versus utilizing expensive security systems."

On February 12, 2007 Sulejmen Talovic shot and killed several people at a shopping mall in Salt Lake City, Utah. Talovic, who was 18 years old at the time, stepped out of his car and immediately began shooting at random as he entered the mall. According to witnesses and police, he tried to shoot as many people as possible. He was armed with a shot gun and wore a backpack full of ammunition. An off-duty police officer, Ken Hammond, who was dining at a restaurant at the mall, quickly responded and cornered the suspect. Several shots were fired between Talovic and Hammond. Talovic was fatally shot after other police officers arrived on the scene. Talovic killed five individuals and wounded several others.

These three incidents demonstrate that shopping malls are easily targeted for criminal activity, whether terrorist related or not. The RAND Corporation released a report on terrorist threats to shopping malls in February 2007. The report stated the terrorist threat to shopping centers is a real concern and confirmed that since 1998 there have been over 60 terrorist attacks against shopping centers in 21 different countries. The authors stated that disaster preparedness plans, which focus on emergency response, do not actively reduce the risk of terrorism. Instead, they recommend that shopping mall owners and security personnel focus more on reducing the risk of terrorism by implementing more stringent security measures to significantly decrease the terrorism risk. For example, the report advised shopping mall employees to periodically train staff to better understand and identify threats such as suspicious packages or possible suicide bombers. In addition, RAND recommends publishing public information around shopping malls to remind people to be on the lookout for suspicious packages. And finally, the report also urged shopping malls to establish emergency response teams, conduct employee background checks and implement photo identification systems for contractors and delivery staff.

The debate continues whether terrorists will target and carry out an attack at a shopping mall. As with most national security concerns, the question remains how much individuals are willing to tolerate in order to protect against a potential threat, and how many resources companies are willing to utilize to do the same. ❖

Regulating Life Sciences Articles in Open Journals

Shannon Michael Allan and
Peter Leitner

The debate over the prevention of biological weapons proliferation, or to paraphrase it, the prevention of the misuse of biological science, has been ongoing for decades. The efficacy of efforts to control tangibles such as production equipment and deadly pathogens, as well as intangibles -- scientific information itself -- has long been the subject of intermittent discussion. The debate on intangibles only acquired "celebrity status" in 2001. Contributing to its increased attention were three distinct events that occurred in that year.[1] These events were followed by the widespread fear that dangerous third parties[2] could potentially use open source publications, such as scientific journals, to develop poor man's weapons of mass destruction to use against adversaries that are more militarily superior.

Three Key Events in 2001

1. Australian scientists modify mousepox to enhance its lethality
2. September 11 attacks on the United States
3. Anthrax letter attacks in the United States

Subsequently, more scientific research was identified and highlighted as potential contributions to bioterrorism. This debate on open publications possibly aiding the advancement of ill-intended third parties' to acquire a weapon with potentially devastating effects was initially confined to a rarified group of specialists.[3] It is only during the last few years that these issues were highlighted by the media and the scope of the discussion broadened. The scope of contemporary concerns today is demonstrated by an article in The Guardian newspaper that reported it was able to get a short sequence of smallpox DNA mailed to a home in London. Further concerns highlighted included the availability of the DNA sequence of the deadly 1918 flu on the internet.[4]

These concerns were addressed generally by legislative initiatives, increased physical security of biological materials, increased scrutiny of student visas[5] and a consensus on controlling open publications that have the potential to aid biological weapons development.[6] In 2004, the U.S. Government created the National Science Advisory Board for Biosecurity (NSABB) following a recommendation by the National Research Council.[7] The NSABB since then has been holding discussions to address this issue systematically and holistically.[8] The NSABB has currently five working groups (WGs) that aim to address and formulate solutions in the areas of Dual Use Criteria, Communications, Codes of Conduct, International Collaboration, Synthetic Genomics and Oversight Framework Development.

All of these actions and discussions were argued to be essential for one main reason – national security, or the NSABB-coined term,"society security." But do all these restrictions truly maintain or strengthen a nation's security? This article will focus on one issue to emphasize the unavoidable complexities that will be faced in addressing this dilemma – the regulation of scientific information in open journals.

Theoretically Optimzing National Security

Since the NSABB was established, it has discussed a number of questions that should be iterated in this article, such as:

> "What is national security? Why is it so difficult to enhance or, perhaps a more appropriate term, optimize a nation's security with regard to scientific advancements? Would controlling information be the best way to maintain or optimize national security? Or would the direct opposite, which could potentially accelerate scientific development, be the best way?"

The NSABB's Dual Use Criteria WG answered the first question on national security by listing the various components that national security includes.[9] For this article, however, Richard Ullman's definition is used to serve the purpose of discussing the complex nature of

(Continued on Page 8)

Journal Regulation *(Cont. from Page 7)*
national security which is described as "an act or sequence of events that threatens drastically and over a relatively brief span of time to degrade the quality of life for the inhabitants of a state, or threatens significantly to narrow the range of policy choices available to governments of a state or to private, non-governmental entities within the state."[10]

In this context, the "act or sequence of events" would be biological attacks. There is no doubt that the use of biological agents against a country would "degrade the quality of life" for its population. Their devastating effects would affect a country's human population, its economy, and its foreign and military policies.[11, 12]

Responsibility to Society

As early as World War I, science has proven to be a "vital force for the advancement or destruction of society."[13] This vital force is controlled by the scientists that research, discover and apply them. Thus withholding or distorting scientific information that could advance the quality of life for a nation would be a great disservice to society.[14] Censoring their work would also be a disservice to both the scientific community and society because "eliminating details about critical methods from scientific publications, [it] compromises [the] ability to replicate and validate results, one of the cornerstones of scientific research."[15] This could ultimately result in going down "false roads because of [the] lack of verifiability."[16] In addition, if results from a particular research project are withheld, it may inadvertently impede the advancement of certain aspects of other particular scientific findings thus slowing down the rate to attaining the full potential quality of life. Furthermore, if regulation of scientific information becomes too much of a burden, it could also lead to scientists deciding to withhold their research results as highlighted by Donald Kennedy, editor of *Science*.[17]

However publishing results with potentially nefarious application would simultaneously allow parties with ill-intent easy access to this information. Thus to publish or not to publish holds a very strong moral dilemma for scientists. Either actions of withholding or sharing could contribute to national security. Thus how would a scientist decide what action to take to ensure his responsibility to society is not compromised?

Scientists' Morale

The other societal issue that could actually be categorized more as an individual concern is the morale of the scientist. A scientist's "professional standing" is heavily dependent on peer recognition and respect.[18] This recognition and respect is acquired through the quality and quantity of their research endeavors which are publicized via publications in journals.[19] Thus scientists "spend considerable time and professional resources in the pursuit of breakthrough information."[20] If upon reaching this goal, their research is banned from publication, it could result in a frustrated scientist as well as having negative consequences for his or her career.[21] This could lead to researchers deciding to "discontinue or not pursue research on regulated biological agents."[22]

Conclusion

Deciding and justifying whether a publication should or should not be published is a complex problem. The main concern of national security cannot be easily satisfied by strictly regulating open journals; however, neither would the threat diminish with the unregulated publication of information which some argue would contribute to advances in biodefense technology.

The extremely difficult task in identifying information that poses a threat to national security is demonstrated by the current effort by the Department of Energy to review millions of archived declassified documents. It is aimed to ensure that information that was declassified under the 1954 Atomic Energy Act, truly does not pose a threat to national security.[23] From 1999 to 2006, 1,736 documents containing about 43 different types and/or forms of information were found to still pose a threat to national security and thus withdrawn from public access. The very act of having to revisit documents that were declassified demonstrates the difficulty in identifying such information and also the need to constantly review the declassification. Furthermore, retracting and re-classifying information could prove to be a fruitless effort as it could already be utilized. The possibility of the current dilemma involving biological research reaching such a state is one's guess.

In the effort to formulate a review
(Continued on Page 13)

Senate Approves Bill to Fulfill 9/11 Commission Recommendations

Senate Homeland Security and Governmental Affairs Committee Chairman Joe Lieberman, ID-Conn., and Ranking Member Susan Collins, R-Me., recently hailed passage of their bipartisan bill to enact remaining or poorly implemented 9/11 Commission recommendations, saying it will help secure the nation against terrorist attacks as well as natural disasters. The Senate approved S. 4, the Improving America's Security Act of 2007, by a vote of 60-38.

"When this bill becomes law, we will have taken a critical step toward building a safer and more secure America for the generations to come," Lieberman said. "This will ensure the American people are better protected against the consequences of natural disasters, such as Hurricane Katrina, than they are today. And we will have done everything possible to make sure no other Americans suffer the loss that so many experienced after the brutal terrorist attacks of 9/11."

"This legislation continues the work of Congress to strengthen homeland security and build upon the 9/11 Commission's recommendations. I believe it will help make our nation safer," said Senator Collins. "Our legislation's broad-front attack on the threats we face will ensure good value for every dollar our nation spends to improve our defenses at the federal, state, and local levels. It will provide appropriate transparency and accountability into the government's security decisions. It will also strike an appropriate balance between increased security and our cherished civil liberties."

S.4 would increase risk-based homeland security grants to states and localities, improve information sharing among all levels of government, restrict terrorists' ability to enter the U.S., and create an interoperable communications grant program for first responders. It also strengthens privacy rights and civil liberties.

Specifically, the bill will:

- Authorize $3.105 billion for each of the next three years for the homeland security grant program to increase prevention and preparedness for terrorist attacks. The grants will be distributed overwhelmingly based on the risk to an area from a terrorist attack. The funds would be allocated through Urban Area Security Grants, State Homeland Security Grants, Emergency Management Performance Grants, and emergency communications and interoperability grants.

- Create a dedicated interoperable grant program within FEMA to help state, local and tribal governments build communications systems that allow first responders from different organizations and different jurisdictions to talk with each other in a disaster.

- Improve the government's ability to disrupt terrorists' travel and infiltration of the U.S. by requiring the Department of Homeland Security and the Department of State to strengthen the Visa Waiver Program (VWP) through improved reporting of lost or stolen passports, requiring countries to share information about prospective visitors who may pose a threat to the U.S., and authorizing an "electronic travel authorization" system through which travelers would apply in advance for authorization to enter the U.S.

- Strengthen the Privacy and Civil Liberties Oversight Board by giving members fixed terms and requiring them to be Senate confirmed; by expanding responsibilities to inform the public; and by providing the board with subpoena power through the Attorney General.

- Establish a voluntary certification program for private sector preparedness to provide companies with a clear roadmap for strengthening preparedness.

- Improve counter-terrorism information sharing within the federal government and among federal, state and local officials by making the Program Manager of the Information Sharing Environment permanent, creating standards for state and local fusion centers, assigning federal intelligence analysts to them, and

(Continued on Page 10)

Legislation *(Cont. from Page 9)* creating intelligence fellowship programs for state and local officials.

Provisions related to rail, aviation cargo, mass transit security, and nuclear proliferation that came out of the Commerce, Banking, and Foreign Relations Committees were melded with the Homeland Security Committee bill on the floor.

"This bill takes an 'all-hazards' approach to homeland security," Lieberman said. "It not only strengthens our defenses against the threat of a terrorist attack, but also prepares all levels of government to respond better to natural disasters such as Hurricane Katrina." ❖

Excerpt: Title XI - Critical Infrastructure Protection

(Sec. 1101) Directs the Secretary to establish a risk-based prioritized list of critical infrastructure and key resources that:
(1) includes assets or systems that, if successfully destroyed or disrupted through a terrorist attack or natural cata strophe, would cause catastrophic national or regional impacts; and
(2) reflects a cross-sector analysis of critical infrastructure to determine priorities for prevention, protection, recovery, and restoration. Requires the Secretary to include levees in the Department's list of critical infrastructure sectors. Authorizes the Secretary to establish additional critical infrastructure and key resources priority lists by sector.

Requires:
(1) each list to be reviewed and updated at least annually;
(2) the Secretary to report annually to the House and Senate homeland security committees and submit with each report a classified annex for required information that cannot be made public; and
(3) the classification of information required to be provided to Congress, DHS, or any other agency by a sector-specific agency to be binding.

(Sec. 1102) Directs the Secretary, for each fiscal year beginning with FY2007, to prepare a risk assessment of the critical infrastructure and key resources of the nation:
(1) organized by sector; and
(2) containing any actions or countermeasures proposed to address security concerns. Authorizes DHS to rely on a vulnerability or risk assessment prepared by another federal agency that DHS determines is prepared in coordination with other DHS initiatives relating to critical infrastructure or key resource protection and partnerships between the government and private sector. Sets forth reporting requirements and provisions regarding the classification of information.

(Sec. 1103) Directs the Secretary to use the National Infrastructure Simulation and Analysis Center, where appropri ate, to carry out the actions required under this title.

(Sec. 1104) Directs the Secretary to report to specified committees for each fiscal year detailing the actions taken by the government to ensure the preparedness of industry to:
(1) reduce interruption of critical infrastructure operations during a terrorist attack, natural catastrophe, or other similar national emergency; and
(2) minimize the impact of such catastrophes.

Barriers to Information Sharing in Homeland Security Partnerships[1]

Amit Kumar, Ph.D.

The author studied the information sharing processes in three homeland security partnerships in the Banking and Finance critical infrastructure sector. The public-public partnership emanates out of the Memorandum of Agreement (MOA) between the Federal Bureau of Investigation (FBI) and the Immigration and Customs Enforcement (ICE) that delineates the jurisdictions of these two agencies with regards to terrorist financing investigations. The public-private partnership comprises two partnerships—the first between the Financial and Banking Infrastructure Information Committee (FBIIC) and the Financial Services Sector Coordinating Council (FSSCC), and the second between the Department of Homeland Security (DHS) and the Banking and Finance Critical Infrastructure Sector. The private-private partnership comprises the Wolfsberg group of private sector global banks that have come together to formulate common anti-terrorist financing and anti-money laundering standards.

Dawes[2] (1996) delineates the barriers to inter-agency information sharing as political, technical, and organizational. The author has examined the political, technical, and organizational barriers to information sharing across the three partnerships and how these may affect the development of these partnerships. These barriers to information sharing are discussed in the following paragraphs.

> "The jurisdictional turf battle between FBI and ICE were political barriers as well as organizational barriers to information sharing. "

The FBI-ICE information sharing process is hampered by political barriers like the greater power and influence enjoyed by the FBI as compared to that enjoyed by ICE. The research found the presence of a feeling amongst ICE officials that the agreement was imposed upon ICE by the powerful FBI. This created barriers to inter-organizational information sharing. Technical barriers to information sharing were being overcome by the establishment of a joint database of cases. Organizational barriers to information sharing like the attitudes of ICE officials (that they possessed sufficient expertise in terrorist financing investigations as an extension of their recognized expertise in financial crime investigations) were observed. The paucity of security clearances, and overtime issues within ICE were another organizational impediment to information sharing within ICE. The jurisdictional turf battle between FBI (the FBI believed it had the requisite expertise in terrorist financing investigations by virtue of its expertise in terrorism through the Joint Terrorism Task Force mechanism and it was thus empowered to take the lead in terrorist financing investigations) and ICE (the ICE officials believed that terrorist financing investigations were an extension of its expertise in prosecuting financial crime cases and it thus had the jurisdiction to investigate terrorist financing investigations) were political barriers as well as organizational barriers to information sharing.

The FBIIC-FSSCC partnership was not hampered by the presence of political, technical, or organizational barriers and this facilitated the information sharing process, thus promoting partnership development. The DHS-Banking and Finance Sector partnership encountered political barriers (the setting up of the Terrorist Threat Integration Center or TTIC outside DHS), technical barriers (the establishment of the Homeland Security Information Network of HSIN-CI and its link to the Financial Services Information Sharing and Analysis Center or FS-ISAC), and organizational barriers (the reluctance on the part of the Banking and Finance Sector to share vulnerability information with DHS, the problems in coordination between Information Analysis and Infrastructure Protection, the lack of security clearances available to Information Analysis officials, and the lack of cyber-security focus within DHS). Such barriers to information sharing within the DHS-private sector partnership hampered the development of the partnership.

The absence of political barriers (the

(Continued on Page 14)

Internet Governance and Security: Exploring Global and National Solutions

May 17, 2007
2:00 pm – 6:00 pm
Swiss Embassy
2900 Cathedral Ave. N.W. (Metro: Red Line, Woodley)
Washington, DC

This symposium on Internet Governance and Internet security will explore the relationship between global and national solutions to problems of cyber crime and cyber security. The meeting will focus on the tensions and complementarities between global and national policy making for issues related to the security and privacy of commerce and communication on the Internet. The panelists and audience are technical experts, academics, and U.S. and international decision-makers in government and industry. They will identify and discuss Internet governance issues such as the security of the domain name system (DNSSEC), spam and cybercrime, identity and identification, and private sector security regimes.

The program is organized by the Syracuse University School of Information Studies; the George Mason University Law School's Critical Infrastructure Protection Program; and the Swiss Federal Institute of Technology at Lausanne.

Panel 1: Securing the Root: The Politics and Economics of DNSSEC
Panel 2: Taking Charge: Public Sector Plans and Private Sector Priorities
Panel 3: National Interest, Global Governance: Which Suits the Internet?

For RSVP, contact:
Kathy Allen
Syracuse University School of Information Studies
kallen02@syr.edu

For more information contact:
Dr. Milton Mueller
Syracuse University School of Information Studies
Mueller@syr.edu

Journal Regulation *(Cont. from Page 8)*
and regulatory process to address this dilemma and a list of pathogens has to be agreed upon, which was proposed to be a combination of the CDC's List and AG List. As for the criteria proposed by the NSABB's working group on Dual Use Criteria, another complementing set of criteria termed in this article "Counter-Balance Criteria" should be used. These criteria would further aid in the decision to allow publication in open journals. Finally, a "Veto Criteria" involving weaponization of biological materials should be implemented.

The method to exchange potentially dangerous information with other trusted researchers in the international community should not prohibit the flow of "contentious research" data. It should divert it to a different route of dissemination, one that is more secure. This process would address the societal issue of ethical responsibility to society and the morale of scientists. Furthermore this regulatory process does not censor the information but keeps it "whole." This could be via the AG's yearly forum or via a restricted access website similar to the "Epi-X" (Epidemic Information Exchange) system. This would also address the issue of international consensus. This is an important concern as we may be inadvertently condemning ourselves to a degrading quality of life while deceiving ourselves into thinking we are depriving bioterrorists of knowledge that unfortunately could be obtained from openly published articles emerging from other countries. Other affected areas of significance could include economic losses and global standing in the field of technology which has political and foreign policy ramifications.

Shannon Michael Allan is a staff officer of the Chemical and Biological Defense Group of the Singapore armed forces.

Peter Leitner heads the Higgins Counter Terrorism Research Center and is a Professor in the National Center for Biodefense at George Mason University. ❖

References

[1] The first was the controversial scientific publication of research conducted by Australian scientists in February. They had modified ectromelia virus (mousepox) in the hope of developing a "virally vectored immunocontraceptive vaccine." The modification, however, rendered the virus "lethal to mice that [were] normally genetically resistant." Scientists in Australia expressed concern with regard to this research saying that "it should serve as a warning to the community to be more aware of the potentially harmful consequences of their work." The other two events that contributed to the aforementioned speculation need no elaboration; the Sept 11 attacks and the closely occurring anthrax letter attacks. - Jackson RJ, Ramsay AJ, Christensen CD, Beaton S, Hall DF, Ramshaw IA. Expression of Mouse Interleukin-4 by a Recombinant Ectromelia Virus Suppresses Cytolytic Lymphocyte Responses and Overcomes Genetic Resistance to Mousepox. J. of Virol. 2001;75(3):1205-1210, Finkel E. Engineered Mouse Virus Spurs Bioweapon Fears. Science. 2001;291(5504):585.

[2] Third parties here would refer to terrorist groups/organizations or countries that the U.S. had listed as possible nations that support terrorist groups or organizations. Terrorist groups such as the Al Qaeda have show to have intentions of using weapons of mass destruction as demonstrated in the May 2003 fatwa, "A treatise on the Legal Use of WMD against Infidels."

[3] Specialist circle in this context refers to the politicians, policy makers and academia that were concerned with such issues.

[4] AFP. Biowarfare from the Net. Today Newspaper, Singapore, 15 Jun 2006. p21.

[5] This is a very valid control as demonstrated during the Cold War, the FSU used postgraduate studies in universities as a form of infiltration and legalization of their spies. These spies would subsequently infiltrate government or other private research institutions that conducted sensitive and secret biological and medical research. – Kouzminov A. Biological Espionage, Special Operations of the Soviet and Russian Foreign Intelligence Services in the West. Greenhill Books, London, 2005.

[6] Knezo G.J. Possible Impacts of Major Counter Terrorism Security Actions on Research, Development, and Higher Education. CRS Report for Congress, 8 Apr 2002, Congressional Research Service, The library of Congress.

[7] The National Academy of Sciences established the Committee on Research Standards and Practices to Prevent the Destructive Application of Biotechnology in 2003. The committee was to "consider ways to minimize threats from biological warfare and bioterrorism without hindering the progress of biotechnology." Its findings recommended a new system that relied "on a mix of voluntary self-governance by the scientific community and expansion of an existing regulatory process that itself grew out of an earlier response by the scientific community to the perceived risks associated with gene-splicing research." One of the recommendations was the establishment of a National Science Advisory Board for Biodefense (NSABB).

[8] U.S. Department of Health and Human Services Press Office. HHS will lead Government-wide Effort to Enhance Biosecurity in "Dual Use" Research. U.S. National Science Advisory Board for Biosecurity. HHS News, 4 March, 2004.

[9] This components would include Public Health, Agriculture, Plants, Animals, Non-biological resources and environment. – NSABB Meeting, Jul 13, 2006. Accessible at http://www.biosecurityboard.gov/NSABB%20Meeting%20Minutes%2013Jul06.pdf on 25 Dec 2006.

[10] Price-Smith AT. The Health of Nations. MIT Press: Cambridge Massachusetts, London, England; 2002.

[11] In the exercise "Dark Winter"; it was estimated that with an initial attack using

(*Continued on Page 14)*

Journal Regulation *(Cont. from Page 13)*
initially infected, there would be 3 million cases of smallpox with 1 million deaths at the end of just one month. In yet another chilling scenario which involved using three different biological agents; anthrax, brucellosis and tularemia, the impact on the U.S. economy was estimated to be in the range of US$477.7 million to US$26.2 billion per 100,000 persons exposed. Milan Brahmatt, the World Bank's lead economist for the East Asia and Pacific Region, estimated that a global human flu pandemic could cause world Gross Domestic Product (GDP) to drop by 2 percent or more which could amount to approximately US$800 billion over the course of a year. - O'Toole T, Mair M, Inglesby TV. Shining light on "Dark Winter". Clin Infect Dis. 2002; 34(7):972-83, U.S. Congress Joint Economic Committee. Terrorist and Intelligence Operations: Potential Impact on the US Economy. Statement by Dr Kenneth Alibek, 20 May, 1998 and Associate Press. Human Flu Pandemic inevitable, says WHO. The Straits Times, Singapore. 2005, Nov 8.

[12] Targeting a country's agriculture with bioterrorism could also result in great economic loss which would include "the value of lost production, cost of destroying diseased or potentially diseased products, and the cost of containment", loss of export markets and associated jobs and even tourism. It was estimated that the U.K. lost approximately £3.1 billion (US$5.4 billion) to agriculture and the food chain in the Foot and Mouth Disease outbreak in 2001. Agricultural producers suffered losses estimated at £355 million (US$619 million) while businesses directly relying on tourism lost approximately £2.7 to £3.2 billion (US$4.7 to US$5.6 billion). - Allan, Shannon Michael and Leitner, Peter. "Attacking Agriculture with Radiological Materials--A Possibility?" World Affairs. Winter 2006, Vol. 168 Issue 3: 99-112, Monke J. Agroterrorism: Threats and Preparedness. Congressional Research Service: The Library of Congress; 2003 and Thompson D, Muriel P, Russell D, Osborne P, Bromley A, Rowland M, et al. Economic costs of the foot and mouth disease outbreak in the United Kingdom in 2001. Rev. sci. tech. Off. Int. Epiz. 2002;21(3):675-687. Available at http://www.oie.int/eng/publicat/rt/2103/3.4.Thompson.pdf #search='United%20Kingdom%20and %20FMD%20and%20economic%20impact'. , accessed on 8 November 2005.

[13] Pigman W, Carmichael E. "An Ethical Code for Scientists". Science. 1950;111(2894):643-7.

[14] Cournand A. "The Code of the Scientist and Its Relationship to Ethics". Science. 1977;198(4317):699-705.

[15] Atlas R. Science Publishing in the Age of Bioterrorism. Academe. 2003;89(5). Available at http://www.aaup.org/publications/Academe/2003/03so/03soatla.htm, accessed on 30 Jan 2005.

[16] Ibid.

[17] Vastag, B. Openness in biomedical research collides with heightened security concerns. JAMA. 2003;289(6):686 & 689-90.

[18] Ferguson J. Scientific and Technological Expression: A problem in First Amendment Theory. Harvard Civil Rights-Civil Liberties Law Review. 1981;16:519-60.

[19] Ibid.

[20] Kellman B. Regulation of biological research in the terrorism era. Health Matrix Clevel. 2003;13(1):159-80.

[21] Atlas R. Science Publishing in the Age of Bioterrorism. Academe. 2003;89(5). Available at http://www.aaup.org/publications/Academe/2003/03so/03soatla.htm, accessed on 30 Jan 2005.

[22] Gaudioso J, Salerno RM. Science and Government, Biosecurity and research: minimizing adverse impacts. Science. 2004;304(5671):687.

[23] In 1999; 45 years later, President Bush signed into law the National Defense Authorization Act for Fiscal Year 1999 (the "Act"). The Act required the Secretary of Energy and the Archivist of the United States to develop a plan to protect against the inadvertent release of records containing Restricted Data (RD) and Formerly Restricted Data (FRD) during the automatic declassification process under Executive Order 12958, "Classified National Security Information." - Federation of American Scientist. Accessible at http://www.fas.org/sgp/news/doeplan2.html on 19 Oct 06.

Barriers *(Cont. from Page 11)*
lack of power differentials amongst member banks), technical barriers (well developed technological systems), and organizational barriers (the lack of a governance structure) to information sharing facilitated the development of the Wolfsberg private-private partnership. ❖

[1] From Kumar, Amit. 2006. The Development of Homeland Security Partnerships: A Comparative Analysis from the Financial Security Arena. Doctoral Dissertation. Washington D.C. © COPYRIGHT By Amit Kumar 2006

[2] Dawes, Sharon S. 1996. Interagency Information Sharing: Expected Benefits, Manageable Risks. Journal of Policy Analysis and Management. 15(3): 377-394

The CIP Program is directed by John A. McCarthy, a member of the faculty at George Mason University School of Law. 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