CIP PROJECT RESEARCH

CIP Project Staff

John McCarthy, *Executive Director*

Emily Frye, *Associate Director, Law and Economics Programs*

Rod Nydam, *Associate Director, Private Sector Programs*

Kevin "Kip" Thomas, *Associate Director, Research Programs / Research Associate Professor*

Dr. John Noftsinger, *Executive Director, JMU Institute for Infrastructure and Information Assurance*

Ken Newbold, *JMU Outreach Coordinator / JMU CIP Project Liaison*

Contact: cipp01@gmu.edu
703.993.4840

If you would like to subscribe to *The CIP Report* please click here.
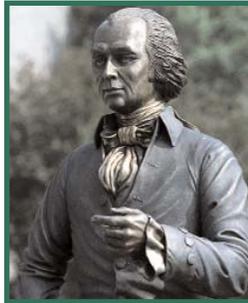
James Madison

Two years ago, the CIP Project began as a $6.5M directed appropriation from the Commerce Committee to develop and implement a broad inter- and intra-university research program that supports public and private sector research needs relative to critical infrastructure and homeland security. To date, more than 70 substantive research projects have been sponsored by the CIP Project including work in direct support of The White House, the Department of Homeland Security, and key industry sectors. The CIP Project funding has grown to over $20M in follow-on grants and has been cited by both the Governor of Virginia and federal homeland security leaders as a model academic program supporting the national CIP agenda.

CIP sponsored research ranges from highly technical efforts to design of new security protocols for cyber systems, to mapping the vulnerabilities of various infrastructures, to exploring the legal and business governance implications of information sharing, to experimental economic analysis.

As the CIP Project enters its third year, we would like to recognize the contributions of Mark Grady. Mark served as Dean of the GMU School of Law from 1997 through summer 2004, and now has chosen to return to his roots in teaching at UCLA. The CIP Project congratulates Dean Daniel Polsby on his promotion to Acting Dean of the School of Law.

GEORGE MASON UNIVERSITY | School of Law
CRITICAL INFRASTRUCTURE PROTECTION PROJECT

This year's new round of research funding will enable the initiation of several exciting projects and the continuation of promising research in the critical

George Mason

infrastructure protection arena. This issue of *The CIP Report* introduces you to the newly funded projects and the names and faces of the professors leading the research. We will keep you apprised of their findings in the coming months.

Sponsored Research Projects

Critical Conversations Series
Digital Right Management of Software Innovations
Proactive Infrastructure Security: Evolutionary Generation of Terrorism Scenarios
The CIP Project Oral History and Digital Archive Project, Phase II
Virus Safe Computing Project
Database of International Law Surrounding Critical Infrastructure Protection
SCIT for Computing and Communications Critical Infrastructure Protection
Assessing the Economics of Maritime Security
Retail Payment System Security: Interbank Systems Managed By Network Operators, Not Banks
Law, Economics, and Technology of Private Enforcement Mechanisms
The Effect of the Tax System on Discouraging Investment in Critical Infrastructure
Strike Season: Protecting Labor / Management Warfare in the Age of Terror
Siting Critical Infrastructure
Economic Analysis of Cyber Security
Private Ordering Solutions to Identity Theft
Private Enforcement Mechanisms for Cybercrime
The Relationship of Public Ignorance to the War on Terror
Energy Regulatory Structure and Insurance Markets
Policyware: Background and Discussion of Open-Source and Proprietary Software
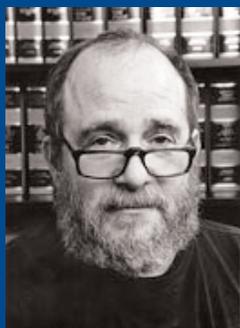
Dean Daniel Polsby Appointed as Acting Dean of the GMU School of Law

Daniel Polsby formally assumes the role of Acting Dean of the GMU School of Law on August 15, 2004. Dean Polsby played a key strategic role in the dramatic ascension to Tier One status of the GMU School of Law. Dean Polsby has also been a staunch supporter of the CIP Project since its inception. Dean Polsby has been a member of the GMU faculty since 1999, where he has taught Criminal Law and Torts and served as Associate Dean for Academic Affairs. Before joining the GMU School of Law Polsby held the Kirkland & Ellis Chair in the law faculty of Northwestern University, where he taught for 23 years. He has held visiting professorships at Cornell, the University of Michigan and the University of Southern California. GMU Provost Peter Stearns has appointed a search committee, chaired by former Federal Trade Commission Chairman Timothy J. Muris. The committee will present a short list of candidates to the university administration by February of 2005.

"The CIP Project is at the very heart of the Law School's plans for the future. The next year should see both a broadening and a deepening of our work."

Critical Conversations Series

Project Lead: Frank Sesno
Professor, School of Public Policy, GMU

Through public discourse of academic research and debate of emerging business and policy actions in the areas of Critical Infrastructure Protection, Cyber Security, and Homeland Security, we are able to raise awareness and work towards practical solutions. These forums and collaborative actions between government, industry, and academia greatly benefits scholarly research. We intend to continue the CIP Project process of collaboration through the partnering of our scholars with leading government and industry actors, as recommended in the National Strategy for the Physical Protection of Critical Infrastructure. The CIP Project's support of information sharing is behind the series of Critical Conversations being moderated by CIP Project Scholar and GMU Professor of Public Policy, Frank Sesno. This will provide for two additional Critical Conversations similar to the previous programs entitled: "Protecting America's Critical Infrastructures: From the War Room to the Board Room" held on June 18th, 2003; "Power Play: Protecting the Nation's Electrical Grid" held on Nov. 19, 2003; and "Turning the Tide: Securing America's Ports" held on June 29, 2004. These were held at the National Press Club where we engaged senior federal, state and private sector executives on the panel discussing their priorities and concerns for ensuring the security of their critical assets and infrastructures.

Digital Right Management of Software Innovations: Policy Evaluation, Strategic Design and implementation

Project Leads:
Taeha Kim, Assistant Professor, School of Management, GMU
Alex Talalayevsky, Asst Professor, School of Management, GMU

Prof. Kim

Software innovations are more vulnerable to piracy, redistribution, and security attacks than other types of innovations. Software developers face a challenging task of protecting software from the development to the commercialization from competing firms, pirate users, talented hackers, virus programmers, or possibly terror groups. Digital rights management (DRM) promises a new hope of software protection. The main question is "How can policy makers incorporate DRM into the current legal system in order to achieve better social outcomes than current situations?" In order to answer the question, an interdisciplinary study of Law, Economics, and Information Systems is needed. First, we will analyze the characteristics of current commercial DRM products. Second, we will set up an economic model to investigate how DRM can collaborate with legal protection systems to result in possibly better outcomes in terms of social welfare, the aggregate of consumer and producer welfare.

The research contribution is threefold. First, predictions and implications out of the economic analysis help policy makers better understand the impact of policy changes and DRM on the social welfare outcomes. Second, investigations provide strategic guidelines for software developers in their implementation of technological protections and legal protections for their

Prof. Talalayevsky

products to be commercialized. Third, propositions provide a design perspective for DRM solution providers by pointing out critical economic and legal issues that their solution characteristics may cause.

The Critical Infrastructure Protection Project Oral History and Digital Archive Project, Phase II
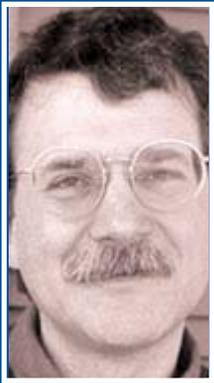
Project Lead: Roy Rosenzweig, Director, Center for History and New Media, GMU
Co-Sponsors/Partners: Kathi Ann Brown, Tom Scheinfeldt, Rebecca Luria

Phase II of the CIP Oral History Project (2 years), will build on earlier work and broaden the collection process, moving on to the period following the release in May 1998 of Presidential Decision Directive 63, the White House's official follow-up to the President's Commission on Critical Infrastructure Protection (PCCIP) recommendations.

Among the key historical events to be explored and documented from this period of intense CIP activity will be the creation of the Critical Infrastructure Assurance Office (CIAO); the work of the Gilmore and the Hart Rudman Commissions; the Y2K turnover process; the lead-up to the events of September 11, 2001; and the creation of the Department of Homeland Security.

In addition to approximately 75 long-form interviews with key policymakers in government and elsewhere, Phase II of the project will produce a multi-faceted digital archive.

Proactive Infrastructure Security: Evolutionary Generation of Terrorism Scenarios

Project Lead: Tomasz Arciszewski, Professor and Chairman
Civil, Environmental and Infrastructure Engineering Department, GMU
Co-Sponsors/Partners: Kenneth De Jong, Mark Houck, Mohan Venigalla, Andrew Sage, David Schum

This project represents a continuation of work initiated under last year's CIP Project sponsored activity "Stage I: Feasibility Study and Building Demonstration Systems." The strategic research objective of this continuing project is to develop a process, an associated set of methods, and computer tools for the generation of terrorism scenarios that will be based on the principles of information technology and knowledge management. The first stage of this initiative was to develop two demonstration systems depicting the nature and feasibility of computer tools for generating terrorism scenarios. This was demonstrated to selected focus groups, emergency management officials, National Guard leadership, and homeland security officials.

As identified in Stage I of this initiative, providing infrastructure security is extremely difficult when dealing with an enemy that is using asymmetric measures-- that is to say an approach that is directed against a nation's vulnerabilities and weaknesses, while ignoring its strengths. Countering this approach requires a great deal of strategic thinking and restructuring to successfully undertake fourth-generation warfare against asymmetric threats - the kind of threats generally posed by terrorist networks.

The proactive approach to security in the face of asymmetric threats calls for the generation of a wide range of terrorism scenarios, the selection of an appropriate scenario to best correspond to an evolving actual situation, and the preparation of appropriate countermeasures. The purpose of this continued study is to develop technology solutions for proactive infrastructure security through the generation of the most dangerous terrorism scenarios.

This stage of the research focuses on

Prof. Arciszewski

continuing the evolutionary design and development of technological solution based principles which synergistically incorporate various aspects of scientific (physical and systems engineering) and computational (computer science) knowledge with evidential reasoning knowledge (scientific law knowledge). This continuing project represents a carefully planned balance between fundamental and applied research, and should produce both novel scientific and very pragmatic results, which afford rapid implementation.
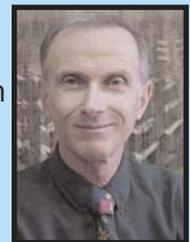
Virus Safe Computing Project

**Project Lead: Jack High
Professor
School of Public Policy, GMU**

Co-Sponsors/Partners: Bill Tulloh, Stephen Rassenti, Anne Marchant, Mark S. Miller

The Virus Safe Computing Project will examine the social, economic, policy and legal factors that will impact the adoption of virus safe computing, and will work with developers of virus safe technologies to ensure these factors are taken into account in designing solutions. The project brings together an interdisciplinary team of researchers with expertise in technology, economics, and policy together with developers of virus safe platforms from industry. This approach can serve as a model of how research into the social factors of cyber security early in the technological adoption lifecycle can inform and enhance the development of useful solutions to the challenges facing cybersecurity. Virus safe computing technology is emerging from research laboratories and moving into commercial production. It is therefore crucial to begin an exchange of ideas between developers of virus safe computing environments and makers of cyberspace policy, to ensure that these technologies meet the broader needs of protecting our critical infrastructure.

Database of International Law Surrounding Critical Infrastructure Protection

**Project Lead: Duminda Wijesekera
Asst. Professor, Center for Secure Information Systems, GMU**

During the next year, The CIP Program will build a database of international law surrounding Critical Infrastructure Protection. The database will initially include identifiable laws and explicit policies from eight key countries regarding cybersecurity, criminal acts related to computer systems, and physical security of national assets, as well as any laws explicitly mentioning Critical Infrastructure. The database will also include laws from other countries to the extent they are already available through secondary resources. The Law and Economics staff at the CIP Project have identified existing sources of relevant international law and policy that will be compiled into a single database. In addition, international law students in the Washington area with core language capabilities in the eight target-country languages will be engaged to perform native-language searches and translations to fill gaps in the core content. JMU and GMU will both serve as testbed entities for database functionality.

SCIT for Computing and Communications Critical Infrastructure Protection

**Project Lead: Arun Sood
Professor, IT & Engineering, GMU
Co-Sponsor/Partner: Yih Huang**

Not all hostile activities can be detected and blocked. We seek technologies to build secure systems which constantly assume that the system may be compromised and perform self-cleansing, regardless of whether the compromise in critical infrastructure is detected or not. We argue that such an assumption is appropriate given the importance of critical communication infrastructures and the sophistication and rapid evolution of information warfare.

A system defense called Self-Cleansing Intrusion Tolerance (SCIT) has been developed. In a SCIT system, a server is periodically assumed to have "failed," namely, compromised by undetected or not-yet-detected attacks. Consequently, the server is brought off-line for cleansing and integrity checking while a backup takes over and assumes the role of the primary server. The newly cleansed system becomes the backup, and the cycle repeats itself. In this proposed project, SCIT survivability will be tested under real attacks. With the understanding of how SCIT responds to various attack tools and attack paths, SCIT can further improve critical infrastructure security.

Assessing the Economics of Maritime Security

Project Lead: Kenneth Button
Professor of Public Policy, School of Public Policy, GMU

The objective of this work is to explore various frameworks that have been developed in the field of industrial organization to help understand the costs of additional security on the maritime transportation value chain.

In particular it would use the structure, conduct, performance paradigm (Mason, 1939) to explore the way that security measures have been applied to the critical elements of the maritime value chain, and their effects on the chain. This would allow for an examination of the pre-heightened security structure of the chain to be examined together with the conduct of actors within it and its economic performance, and then explore how actual changes that have taken place have impacted on the chain (the 'market period effect') and to examine in a quantitative and qualitative way, using scenario analysis and subjective quantitative assessments, the likely longer term implications for the chain as security related transactions costs etc. increase over time. The usefulness of using a generalized structure, conduct, performance framework in combination with Porter's value chain is that attention can be focused on a single output - the profit margin. This obviously misses important social considerations but it can provide a basis for the subsequent development of tractable cost-benefit techniques for assessing the value of various security initiatives.

Retail Payment System Security: Interbank Systems Managed By Network Operators, Not Banks

Project Lead: Neil Murphy
Professor, Virginia Commonwealth University

The network operator in retail payment systems in the United States is, in some cases, the Federal Reserve System (check clearing and the automated clearing house system), private banks (check clearing through correspondents), and non-banks (bank credit cards and ATM/debit cards). Bank supervisors are charged with examining the adequacy of a bank's systems and procedures for managing obligations arising from their customers' transactions. However, a bank may have fulfilled all the requirements for a well managed process, including its connection to the network, but it can be at risk from difficulties occurring at the network level.   If all these networks must compete, and pay close attention to their costs of operation, then what are the incentives for them to expend the necessary resources to secure the networks? The networks take advantage of network externalities which imply that the private benefits of participating depend not only upon an individual bank's calculus of costs and benefits but whether or not many other banks, merchants, and consumers find the network product to have net benefits. In such a case, it is difficult to know exactly how to allocate costs to members of the network, especially those costs which cannot be easily associated with benefits to an individual participant. The purpose of this proposal is to review the existing arrangements for payment system network security in light of these concerns.
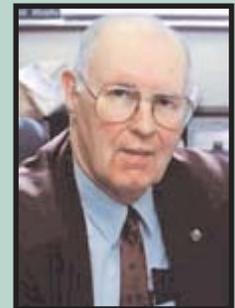
Law and Economics: A Dynamic Research Agenda for Changing Times

This second year of Law and Economics programming is generating novel ideas and extensive new thought leadership. The current set of projects is diverse, and ranges from pure theory to pure application, including everything in between. Following is a brief summary of our current Law & Economics projects.

The CIP Project remains the only institute in the nation examining the legal issues associated with Critical Infrastructure Protection. As the first round of sponsored research ripens, and the second develops, the fruits of such a dedicated program are becoming increasingly apparent. The topics presented by law scholars has led, further, to an abundant list of legal, economic, and policy issues that deserve exploration. The challenge is in limiting and prioritizing the work to be done.

The Law and Economics of Cybersecurity

Bruce Kobayashi , GMU School of Law

This project, ongoing from 2004 through 2005, provides a legal and economic analysis of security standards on computer networks, and for sanctions for non-compliance with such standards. To date, the project has resulted in two concepts that will be developed further with the next round of funding. The work through July 1, 2004, will be published in book form during the next calendar year.

Law, Economics, and Technology of Private Enforcement Mechanisms
Peter Boettke, James M. Buchanan Center for Political Economy

Since in our capitalist economy most resources are privately owned, industry security and national security are inextricably linked. If businesses were unable to conduct commerce over the Internet or to protect their property from attack, the economy as a whole would be extremely vulnerable. But fortunately the incentives of private enterprise are to increase commerce and to protect property, which is aligned with protecting the security of the nation. With these issues in mind, this project concerns a vast variety of topics dealing with the cyber-economy and the law, economics, and technology of private enforcement. The range of issues covered by this project will result in a symposium series during Academic Year 2004-2005, and will be compiled in book form in 2005.

The Effect of the Tax System on Discouraging Investment in Critical Infrastructure

Terrance Chorvat, GMU School of Law

This project analyzes the tax regime and suggests modifications to enhance insurance coverage options for critical infrastructure.

Energy Regulatory Structure and Insurance Markets
Ed Flippen, McGuire Woods, LLP

This project analyzes the role that insurance policy plays / can play in enhancing efforts to protect critical infrastructure.

The Relationship of Public Ignorance to the War on Terror
Ilya Somin, GMU School of Law

Since September 11th, a number of legal scholars have argued that limits on federal power to force states to cooperate inhibit the war on terror. This paper analyzes whether there is cause to expand Congress' general Commerce Clause powers over the states, in light of the power already granted to Congress under the War Powers Clause. Furthermore, the paper examines whether there is any reason to believe that state governments would, on average, do a worse job of providing security voluntarily than the federal government.

Strike Season: Protecting Labor / Management Warfare in the Age of Terror

Ross Davies, GMU School of Law

Outside of the issues of workplace violence and sabotage, neither the NLRB, nor the courts, nor Congress have paid much attention to the relationship between public safety and labor-management conflict in the private sector. Furthermore, neither the National Labor Relations Act (NLRA) nor common federal labor law directly addresses or resolves the problem of reconciling evolving concerns about critical infrastructure protection with strong traditions of wide latitude for labor and management to take mutually harmful action. This paper takes attempts to develop a constructive solution to the problem of strikes and infrastructure protection.

Siting Critical Infrastructure

Steven Eagle, GMU School of Law

In addition to technical considerations and direct national security threats, an important problem in the transmission of both energy and data is the lack of adequate distribution grids. This difficulty is largely a product of structural inadequacies in land use regulation. Legislators at all levels must, and currently are, undertaking to reform land use regulation. This research analyzes the constitutional implications of these reforms and generates alternatives to command-and-control regulatory models for siting critical infrastructure assets.

Policyware: Background and Discussion of Open-Source and Proprietary Software

Thomas Wingfield & Emily Frye

This ongoing project examines the relationship of open-source and proprietary software to national security.

Private Enforcement Mechanisms for Cybercrime

Michael O'Neill, GMU School of Law

This paper examines the potential use of private enforcement mechanisms to police and prosecute cybercrime. The historical roots of government monopolization of the investigation and prosecution of criminal offenses is explored, and contrasted against modern experience with cybercrimes, in which private industry often has far greater experience and financial resources than government to investigate crimes committed against them on the Internet.

Private Ordering Solutions to Identity Theft

Michael Krauss GMU School of Law

The fundamental question of this paper is why tort law has seemingly been unable to adequately address identity theft. The issue of "credit bureau immunity," often a product of rent-seeking statutes, may have thwarted the common law. This paper contends that the removal of such statutes might serve to invigorate private ordering, in a field rapidly taken up by proliferating regulatory bureaus.

LEGAL INSIGHTS

by Emily Frye

The Law and Economics of Cybersecurity: Architecting for Protection

On June 11, seven of the nation's leading Law and Economics scholars gathered at GMU School of Law to present their work on cybersecurity, which the CIP Program sponsored over the past year.

Mason's own Bruce Kobayashi offered the keynote, setting the bar on fundamental analysis of how Law and Economics can add value in policy approaches to cybersecurity. Yochai Benkler (Yale/ of Coase's Penguins fame) argued that some of the Internet's surge problems during crises can be solved by enabling rapid deployment of highly localized unused capacity resources, as was done after 9-11 in New York. Amitai Aviram (Florida State) clarified how patterns of group behavior shed light on why some ISACs function more efficiently than others, and how knowledge of these patterns can be used to promote healthy ISAC growth in the future. Peter Swire (Ohio State) demonstrated that network security models incorporating unique features are more likely to benefit from security-feature concealment, while networks deploying widespread or common elements benefit from openness. Joel Trachtman (Tufts) posited the usefulness of an international governing body for standards in Internet operation, arguing that jurisdiction can serve as a method for establishing congruence between risk and control in the Internet space.

Most interesting, though, was the interplay of three papers from dramatically differing points on the philosophical spectrum. The papers were developed independently, and the authors would not generally share the same perspective on legal issues. Yet a common theme emerged in all three: the key role that structure plays in Internet security.

The Dark Side of Private Ordering: The Network/Community Harm of Crime, by Neal Katyal (Georgetown) presented persuasive evidence that the architecture of Internet space, like physical architecture in real space, has a profound effect on behavior within that space. Katyal's premise reverberates as well the messages presented by Randy Picker, Eric Posner, and Doug Lichtman (all at the University of Chicago). Picker questioned the now well-known "biodiversity theory" of Internet resilience - that is, the idea that Internet operating systems should mimic a healthy ecosystem. Creating, deploying, and interoperating mul-

tiple operating systems, argued Picker, is a very expensive proposition. Instead, might it be more cost-effective to instill principles of autarky[1] into high-value systems? Certain systems are so critical that they should be (separated or separable from) the Internet at large. Picker's thinking is counter to trends in recent years, which have led to SCADA and financial management systems linking directly into the Internet backbone. Perhaps those integrating key systems have expected the importance of the functions now running on the Internet to result in the development of heterogeneity. Whatever the reasoning, meaningful heterogeneity is nowhere in sight. In the absence of heterogeneity or alternative approaches to securing the Internet, vulnerability is at record levels and increasing.

Posner and Lichtman presented a paper on ISP liability. They responded to a

Presenters at the June 11 Law and Econ Conference

Writing History in Cyberspace: The CIP Oral History and Digital Archive
by the CIP Oral History Team*

The Critical Infrastructure Protection (CIP) Oral History Project is gathering fascinating and revealing insights into the historical roots of current CIP policies. The Project seeks to a create a comprehensive archive of oral history interviews with key figures in the critical infrastructure story and to use those interviews (and other documents) to write an accessible history tracing the evolution of U.S. critical infrastructure protection policy.

"One of the unexpected outcomes [of the 1987 Senate hearings on terrorism and the risks of terrorism in the U.S.], I believe, was a beginning realization of the threat represented by information technologies and the extent to which information technologies might be an easier target to damage than the physical infrastructures they controlled."
-Oral History Participant

This year we are focusing on gathering interviews on the historical roots of CIP and especially the developments that led to Presidential Decision Directive

63. In future years, we will look, for example, at creation of the Critical Infrastructure Assurance Office, the events of Y2K and the eventual establishment of DHS.

By speaking with former Commissioners and staff from the President's Commission on Critical Infrastructure Protection (PCCIP), we are learning how thinking about issues such as interconnectedness, infrastructure assurance and private/public partnership have evolved with the emergence and ubiquity of our information technology capabilities. We have heard about the deliberations involved in drafting their influential final report, Critical Foundations; prior efforts by various government agencies represented on the Commission to address the emerging vulnerability of infrastructures; and past events that have influenced the course of policymaking by national leaders.

We have also interviewed others who were closely associated with the PCCIP, such as members from the Critical Infrastructure Working Group (CIWG) and congressional leaders. But the 'CIP Story' involves much more than Presidential Commissions and national security leaders. Many other critical infrastructure practitioners have inherited the foun-

dation created by the PCCIP and have worked at implementing many of their recommendations. In order to document that story, we need to hear from you.

"The Commission was absolutely unique in that most commissions are established in response to something horrible happening. We established the President's Commission for Critical Infrastructure Protection but nobody had attacked critical infrastructure yet. We were ahead of our time. But because we were established a little bit on the earlier side, there was less embracing [of our recommendations and findings]."
-Oral History Participant

We have teamed up with the Center for History and New Media (CHNM) at George Mason to tap into their expertise of conducting "virtual oral history." CHNM has been involved in several projects devoted to capturing the recollections of participants in key moments in recent history. One popular (Continued, Page 14)

Roy Rosenzweig - GMU Department of History, Tom Scheinfeldt - GMU Center for History and New Media 9/11 Digital Archive, Kathi Ann Brown - Milestones Historical Consultants and Rebecca Luria - CIP Oral History Project

Private Efficiency, Public Vulnerability:
Developing sustainable strategies for protecting critical infrastructure

A group of thirty critical infrastructure experts from government, industry and academia met in Cambridge, MA, for a workshop co-hosted by George Mason University and the Kennedy School of Government (Harvard University) titled "Private efficiency, public vulnerability: Developing sustainable strategies for protecting critical infrastructure." The May 27-28 workshop and related activities, funded by a grant from the Critical Infrastructure Protection Project, are intended to inform development of public policies and business strategies that are both effective in enhancing the resilience of critical infrastructures, and economically and politically sustainable in the long term. Developing such policies and strategies is particularly difficult in specific contexts where the drive for efficiencies in infrastructure operations increases inherent infrastructure vulnerabilities.

Workshop participants included Alfonso Martinez-Fonts, Jr., special assistant to the secretary for

the private sector in the U.S. Department of Homeland Security; Harris Miller, president of the Information Technology Association of America; insur-

ance industry executive Jim MacDonald, executive vice president of ACE USA; Franklin Nutter, president of the Reinsurance Association of America; Stephen Flynn, Jeane J. Kirkpatrick Senior Fellow in National Security Studies at the Council on Foreign Relations; Todd R. La Porte, Professor of Political Science at UC Berkeley; Geoffrey Heal, Paul Garrett Professor of Public Policy and Business Responsibility at Columbia University Business School; and Howard Kunreuther, co-director of the Risk Management and Decision Processes Center at the Wharton School.

The conference was jointly organized by GMU faculty members Philip Auerswald and Todd M. La Porte and Kennedy School professor emeritus Lewis Branscomb. The organizers will work with participants over coming months to produce a workshop report emphasizing policy options that will be released in January 2005. They also are planning a university press book that will follow the structure of the workshop and will include chapters by the organizers and papers contributed by the participants. ❖

George Mason University
Graduate Certificate in Civil Infrastructure and Security Engineering

The graduate certificate in Civil Infrastructure and Security Engineering is a professional program that is appropriate for civil infrastructure (transportation, water and wastewater, utilities, etc.) owners and operators, designers, planners, maintenance staff, and other technical workers within the public and private sectors, who are responsible for improving facility and equipment performance, reliability, security, efficiency, and management practices.

New approaches to civil infrastructure problems are emerging that use traditional civil engineering domain knowledge, in the context of information technology with a systems approach, to analyze the complexity of and interaction among various infrastructure components and their performance. Currently, the most important challenge of infrastructure engineering is to improve the quality of stewardship, which falls far short of public expectations, and to improve immediately the security of critical civil infrastructure. The Civil Infrastructure and Security Engineering Certificate is intended to respond uniquely to the need for broad training in the holistic/systems approach to the long-term management of infrastructure, with specific attention to risk and vulnerability assessments, and to creative solutions to providing improved system security. The certificate program is flexible and can be tailored to the needs of students within the infrastructure engineering community, but is also intended to be responsive to the needs of infrastructure owners, operators, and other technical staff.

Admission Requirements

Potential candidates should have a bachelor's degree in Engineering, Architecture, Mathematics, Science, or other related technical field, and must also be computer literate. Candidates should inquire with the certificate coordinator for details of program planning. Courses are offered in late afternoon and evening and are particularly suitable for part-time students.

Certificate Requirements

The certificate program consists of 15 credits (five courses), selected from certificate program courses and elective courses. The certificate courses are aimed at building the foundations of asset management methods based on a holistic/systems approach. The certificate program courses consist of:

One core course, CEIE 680, Introduction to Infrastructure and Security Engineering (3 credits)

A minimum of two of the following specific sector courses:
- CEIE 681 Security of Structural Systems (3 credits)
- CEIE 683 Water and Wastewater Systems Security (3 credits)
- CEIE 686 Transportation System Security and Safety (3 credits)

The planned schedule for offering the above courses is as follows:
- CEIE 680 Fall 2004, Spring 2006
- CEIE 681 Spring 2005
- CEIE 683 Spring 2005
- CEIE 686 Fall 2005

The remaining elective credits must be selected from the following course listing:
- CEIE 510 Geographical Information Systems in Engineering
- CEIE 511 Design and Inventive Engineering
- CEIE 670 Civil Engineering Decision Methods and Tools
- CEIE 671 Best Engineering Management Practices
- CEIE 685 Civil Engineering Information Management
- CEIE 690 Special Topics (depends on the topic; requires coordinator approval)
- PUBP 710 Pricing, Management, and Privatization of Public Assets
- PUAD 640 Public Policy Process
- PUAD 661 Public Budgeting Systems

Selection of courses is subject to the approval of the certificate coordinator to ensure cohesiveness and compatibility. Some courses may have prerequisites for which the student must qualify or seek a waiver from the appropriate instructor. A cumulative GPA of 3.000 is required, and no more than one course with a grade of C may be applied toward the certificate.

M.S. in Civil and Infrastructure Engineering

To earn the M.S. degree, with a specialization in infrastructure management, students would complete an additional 12 credits of course work, a 3-credit project, and a minimum of 10 graduate seminars approved by the CEIE department for the degree program.

Contact:

George Mason University
Dept. of Civil, Environmental & Infrastructure Engineering
Attn: Dr. Michael Bronzini
Science & Technology II, MSN-4A6
Fairfax, VA 22030
Tel. 703-993-1504
mbronzin@gmu.edu

In Memoriam
John L. Burke Jr., 1945 - 2004

The CIP Project notes in sadness the passing of an important and key player in the critical infrastructure protection arena. John Burke Jr., a Washington corporate and real estate lawyer, died June 26 of brain cancer. He was 58.

Mr. Burke was managing partner of Foley Hoag, LLP, where he specialized in corporate and real estate matters, and more recently in the law of electronic commerce. His clients included large financial institutions, law firms, and government agencies. Mr. Burke was active in crisis management coordination, with a particular focus on issues of interdependencies between the finance sector and other critical infrastructure sectors such as telecommunications.

He founded "Where It's Needed," a charity to combat homelessness, and was a member of the Washington Lawyers' Committee for Civil Rights and Urban Affairs for 30 years, twice winning the group's outstanding achievement award. He was also an adjunct professor of law at Georgetown, specializing in ethics and professional responsibility.

Mr. Burke, a native Washingtonian, graduated from Fairfield University in 1967 and received a law degree from Georgetown University in 1971.

John was a good friend and supporter of the CIP Project and his passing is felt on many levels.

Oral History (*Cont. from Page 10*) project is the September 11th Digital Archive, which has collected more than 16,000 personal accounts and 130,000 digital objects which tell the story of that day.

The CIP Oral History Project would like to do something similar, but on a smaller scale. But we need your help. We're interested in hearing your stories as well as the stories of your colleagues and associates working in the field of critical infrastructure. Please visit our website (http://echo.gmu.edu/CIPP/) where you will find a description of the project, members of the research team and a survey that asks about your own role in and views about critical infrastructure protection. With your participation, we will be able to craft a well-rounded historical narrative and leave a complete historical record. But without your participation, the story will be incomplete.

Please visit our website and contribute to the story. ❖

Note: To view and contribute to the September 11th Digital Archive, please visit: http://911digitalarchive.org.

Legal Insights (*Cont. from Page 9*) question about international legal frameworks for liability by suggesting a structural division between assertedly high-security players and others. Internet traffic makes many hops between sender and receiver, and the origin of a piece of digital material is impossible to determine. The final hop, however, can be identified by the U.S.-based ISP. In theory, ISPs here could refuse to accept material from countries that fail to subscribe to security standards. If we lock out traffic from "bad" countries, we could safe- guard the operational integrity of a U.S.-based backbone and network. Over time, an increasing number of international ISPs might see the benefit of subscribing to security standards as greater than the cost, and the safe space would become the heavyweight. In order to accomplish any substantial business, a country (or its ISPs) would have to buy in to the rules of the dominant players.

An unexpected thread ties these pieces together: structure shapes action. The Internet was built for simplicity, but the stakes have risen. We're too far along to discard the existing backbone. Yet the vulnerability of this, the ultimate Critical Infrastructure, jeopardizes our economy, national security, and - beyond our borders - progress in the world to which we are linked. With all this at stake, we need to find the resources for architectural reinforcement. ❖

[1] "Autarky" is the economist's term--and spelling--for independence of operation.