The CIP Report

VOLUME 1, ISSUE 4 SPECIAL EDITION OCTOBER 2002

Message from John McCarthy, Executive Director, CIP Project

John McCarthy

This special edition of the CIP Report provides you with an update on the CIP Project's ongoing research activities and significant events. Also, I have included a section in this newsletter titled "CIP Project Focus" that provides you information on our overall objectives. As we move forward, we continue to develop a deeper appreciation and understanding of the interdependencies of law, policy, and technology in providing for critical infrastructure protection and cyber security.

The CIP Project has begun work on our initial research projects, which have already received significant attention from government and industry. Specifically, we have received strong support and interest in our research on Internet infrastructure vulnerabilities. Our plans for assessment of network interdependencies and cascade effects have been endorsed by the Department of the Navy and the National Defense University. In addition, we are beginning work with George Mason University's Interdisciplinary Center for Experimental Science (ICES) on a project to assess underlying economic incentives. Work is beginning on several significant legal research projects focusing on private ordering solutions to cyber security, and legal impediments to information sharing. Finally, the GMU School of Law completed a very successful conference focusing on Cyber Crime involving over 100 senior legal scholars and professionals across the country.

Solid working relationships with our James Madison University partners have been established in pursuing the technical aspects of our research. Most significantly, we have received strong support from JMU who is taking the lead in developing a project web presence for both universities. Also, professors from both universities are getting involved in research activities such as defining necessary elements of network security risk assessment systems and procedures.

The CIP Project's efforts in developing key relationships within government and industry have been very productive as well. We have provided several presentations to senior government officials on our evolving research on information infrastructure capacities and vulnerabilities. We have continued to support the insurance industry in their efforts to develop methods of costing cyber security. And, we have forged relationships with infrastructure owner / operators as well as leading cyber security service providers, in order to gain insight into industry specific concerns and to build partnerships in our efforts to provide practical solutions.

Leading congressional voice on terrorism, Congressman Frank Wolf, discusses critical infrastructure at the GMU School of Law

THE TECH CENTER
National Center for Technology & Law
CRITICAL INFRASTRUCTURE PROTECTION PROJECT

We have made excellent progress in integrating the disciplines of law, policy and technology to enhance our nation's critical infrastructures and cyber security. This has been made possible only through unprecedented levels of cooperation and sincere commitment by all involved who are working toward this common goal.

As noted above, this special edition of the CIP Report provides you with an update on CIP Project research activities and significant events. I intend to periodically provide you with similar special editions to update you on key project activities. This edition includes:

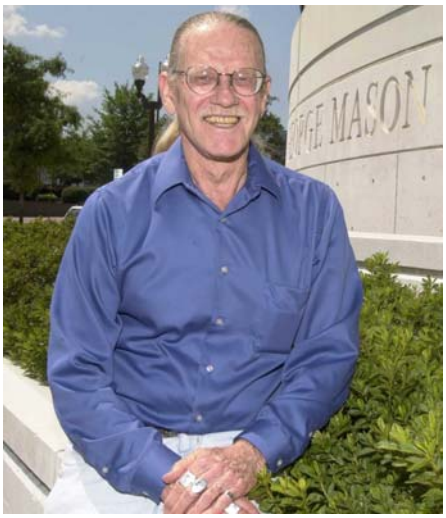
- Spotlight on Excellence – Recognizing Dr. Vernon Smith's significant achievement in earning this year's Nobel Prize in Economics;
- CIP Project Focus--Current focus of CIP research efforts;
- CIP Project Highlights – Summaries of research projects underway;
- CIP Project Scholar's Analyses – A scholarly discussion concerning infrastructure interdependencies, and assessment of the recent attack on the internet root servers.

In addition to these featured items, throughout this edition are quotes from members of our CIP Community who are lending their voices to the debate.

Spotlight on Excellence

Vernon Smith, Professor of Law and Economics at George Mason University and Distinguished CIP Project Scholar, Wins the Nobel Prize in Economics

The Royal Swedish Academy of Sciences announced on October 9, 2002 that Dr. Smith will receive the 2002 Nobel Prize for Economics. Smith will share the prize with Princeton psychology professor Daniel Kahneman.



Vernon L. Smith was born in the flat plains of Wichita, Kansas during the boom years preceding the Great Depression, January 1, 1927. Born to politically active parents--an avowedly Socialist mother who revered Eugene Debs-- Vernon Smith's early ideological indoctrination would prove pivotal to his attraction to the economic sciences.

While earning his bachelor's degree in electrical engineering at the California Institute of Technology in 1949 Smith took a general economics course. Intrigued, Smith pursued the science, receiving a Masters in Economics from the University of Kansas in 1952 and a Ph.D. from Harvard University in 1955.

Dr. Smith's initial training in the hard sciences lead him to pursue the application of the scientific method in his chosen profession, and social science, of economics. Predisposed to have the heart of a socialist, Dr. Smith expected to prove the inefficiencies of market mechanisms when he conducted his first economic experiments in 1956 at Purdue University, using his students as subjects. However, Dr. Smith's experiments--testing economic concepts and theories under controlled conditions--instead overwhelmingly demonstrated to him the clear efficiencies of markets. Smith found that even with very little information and a modest number of participants, subjects converge rapidly to create a competitive equilibrium.

Specifically, Smith's experiments proved large numbers of perfectly informed economic agents were not prerequisites for market efficiency--a radical departure from conventional economic thought. Smith compiled his early experiments and in 1962, while a Visiting Professor at Stanford University, published his findings in the *Journal of Political Economy.* The article, "An Experimental Study of Market Behavior," is today considered the landmark paper on experimental economics.

Over the years, Dr. Smith has become well known as an expert in capital theory formation and an early pioneer in the field of environmental economics. He has done research and taught experimental methods at universities across the country, and has published numerous seminal works exploring, and defining, experimental economics as well as other economic disciplines.

In 2001, Dr. Smith and six colleagues formed the Interdisciplinary Center for Experimental Science (ICES) at George Mason University. At ICES, Dr. Smith and his colleagues continue to conduct economic experiments and solidify the application of developed knowledge. Current research is focused on the design and testing of markets for electric power, water and spectrum licenses. Dr. Smith and his colleagues have also worked with the Australian and New Zealand governments on privatization issues, developed market designs for the Arizona stock exchange, and designed an electronic market for water in California.

Dr. Smith's groundbreaking work has led to an explosion in the application of laboratory experimental methods. Volumes of experimental papers are being published each year and the number of experimental laboratories is growing rapidly around the world. ICES is now the preeminent facility serving as a model for experimental economic and laboratory development throughout the world.

Interview with Professor Vernon Smith

by Frank Sesno

Q: Congratulations on winning this year's Nobel Prize in Economics. What first went through your mind when you were informed of this incredible honor? How has it changed your life and work?

A: I felt incredible relief. Because my friends had predicted for over twenty years that I would win the Nobel Prize and now I didn't have to worry about them anymore. It's changed my life because I travel more but not much more yet. And for work, now I get higher fees. But because all fees – including the Nobel Prize amount – go to the International Foundation for Research in Experimental Economics (IFREE) to fund our research I don't feel so guilty about accepting higher fees.

Vernon Smith discusses his research with Frank Sesno.

Q: You have proposed research to examine the impact of increased competition from alternative energy reserve prices and security levels. This scenario would require significant changes to our energy infrastructure. What are the economic legal and regulatory implications of changes to the high voltage grid?

A: By allowing freer entrance for alternative energy providers at the retail level. The trick here is to keep local wire distribution and innovation at differing prices. No one knows how that should be valued, so we need the market to create competition. To date, local utilities have operated to serve all customers at a fixed price. Regardless of priority or need – for example a hospital – all energy users receive the same priority of service. If the hotel or airline industry were forced to operate in this same manner, cities would consist of only hotels, and airports would be filled beyond capacity with surplus airplanes.

Currently the FERC looks at the energy problem at the grid level. It's like looking through the wrong end of a telescope. Down at the retailer level the local franchisee cannot separate energy demand because of this effective wire monopoly. This is just like Microsoft selling their software bundled with the operating system. When they do it, it is illegal. A further problem is the differing laws that states impose on electrical distribution.

At the retail level, allowing individual appliances to be interrupted based on some contractual arrangement allows for more surplus based on demand responsivity. Actual interruptions of demand allow for greater efficiency and the balance of potential interruptions allows a measure of reserve, allowing for enhanced security.

Q: Given the need to protect the country's critical infrastructure, how can the free market ideas you have articulated contribute to increased security for the energy sector?

A: Interruption below the substation level, at the individual appliance level, allows you to keep the grid up by reducing non-vital demand. Instead of shutting down everyone in Chicago you can still allow vital loads downstream to operate by prioritizing these demands.

Security, Efficiency and Pricing Performance of Enhanced Electric Power Markets

This project would entail the development of new software designed to conduct a wide range of human subject trading experiments for electrical energy on the high voltage grid. This will allow for an in-depth study of demand side incentives and market trading rule restructuring enabling security and reliability to be priced along with energy in the interests of improved efficiency and robustness to both natural and terrorist-induced outages.

We propose to evaluate the market and security impact of different mixes of supply or demand side responsivity. The methodology is that of the controlled laboratory experiment using trained, profit-motivated subjects. In effect the research will evaluate market feasibility, the effect of demand responsivity on energy reserve prices, and security levels. In particular the research will enable one to measure the reduced impact of outages on the involuntary loss of service where calls on voluntary demand interruption substitute for supply side reserves.

The barriers to changes to the high voltage grid are legal and complicated by a regulatory mind set. Local distributors have a franchised monopoly over the wires and their incentive is to tie the sale of energy in with the rental of the wires. But, energy is separable from the wires, and can be provided competitively by alternative energy providers.

This research initiative is intended to explore the feasibility of increased security through demand side reserves. The hypothesis to be evaluated is whether demand side reserves increase the efficiency of energy delivery, control price volatility and generator market power, and reduce vulnerability and cost of power outages.

Economic Modeling of Cyber Security

Expert observers of information networks raise the following question: Given the inherent security externalities created by connected networks of information providers, does the system as a whole provide an optimal level of security? While this question is important, it is difficult to answer in practice because of the inherent privacy of firm specific information, such as expenditures on, and implementation of, security procedures and technologies as well as the value of information available at other nodes and the extent of potential (or reported) damages caused by the exposure of information to the network. We use experimental methods to provide a replicable information network environment where we can study the behavior of cash motivated decision-makers.

Optimal security involves a tradeoff between investments in securing information on the network and deciding what information to expose to the network. In general the greater the amount of information exposed, the greater the economic value of the network. At the same time, more information increases the risk of greater damages if the network is compromised. Within this framework we study the institutional rules whereby individual decision-making, based on private information, can lead to the optimal provision of network security and economic value.

Within a well defined, value induced, information network we look at two key decisions that produce network externalities on others:

1. How much to invest in information security.
2. Level of risk in terms of potential damages from information exposure.

Within our environment we can define the tradeoff between expected benefits and losses for given security, and hacker, technologies. Given this tradeoff we can define as a benchmark the set of decisions that would maximize economic value. Given this calculation our immediate goal is to study the degree to which individuals can self-insure through a network of bilateral contracting on mutual damages, and the degree to which standard insurance contracts can be used to create markets to share risk and still provide optimal value. Answers to these questions will define a research program that will allow us to design ‘smart’ combinatorial market solutions for a decentralized market solution to network security that can include decision-makers who are representing national interests.

Our initial research is designed to answer a number of difficult research questions that may have a significant impact on actual practice. These questions include the following: How do we design experiments that appropriately reflect real world networks? How do we collect data and define and make measurements in an inherently stochastic dynamic system? How do we perform statistical hypotheses testing and estimation in a stochastic and dynamic network environment?

CIP Project Focus

- Provide thought leadership around complex cyber security issues and offer solutions for critical infrastructure issues that benefit both Government and Private Sectors with particular focus on market based solutions.
- Address information sharing impediments, whether legal, business, or technological, that undermine collaboration for enhancing cyber security and critical infrastructure collaboration.
- Produce research for senior business and policy makers that explores the relationship between critical infrastructure and homeland security, including more useful business models that implement policy solutions.
- Focus resources on supporting Information Sharing & Analysis Centers (ISACs), emphasizing legal and business solutions that facilitate more profound information collection, analysis, and dissemination.
- Develop new technological and business solutions that improve cyber-security and risk management within our nation's academic and research institutions.
- Explore insurance and risk transfer solutions as a means of enticing superior risk management behavior in the nation's critical infrastructure and business communities.
- Support research that leverages modeling, simulation, and mapping of complex critical infrastructure challenges – these especially include infrastructure interdependencies as well as downstream and cascading damages that offer insights for senior policy and decision makers.
- Support advancement of the international critical infrastructure agenda through research and partnering activities; multiple countries have already expressed an interest in collaborating with the GMU CIPP, including Canada, New Zealand, the Netherlands, and Australia.
- Support the proliferation of critical thought in the areas of cyber security and critical infrastructure protection, including an emphasis on scholarly research as well as symposium and workshops.

Dr. Linwood Rose, President,
James Madison University

"I am excited to see the work being done through the Critical Infrastructure Protection Project at James Madison University and George Mason University to help secure the nation's most vital interests. As a member of the National Infrastructure Advisory Committee, I realize the importance of collaboration and cooperation in this area and am pleased that these two universities are working together."

Dr. Alan Merten, President,
George Mason University

"Northern Virginia is increasingly becoming an international leader in information-based technologies, but the greatest threat to these exciting technologies, and the government agencies and private companies that depend upon them, is the security and stability of the underlying information. The CIP Project provides a center for the ideas that will protect the nation's information resources."

CIP Project Highlights

Private Ordering Approach
Led by Dean Mark Grady and Amitai Avarim

The Private Ordering Project plan involves a detailed study into the law and policy incentives that are necessary to allow for effective and efficient means of providing cyber security. The basic approach is to focus on privately ordered solutions. The Private Ordering Approach is identifying the key researchers in the areas of cyber insurance, cooperatives, civil liability, CIP, and cyber crime. Through a series of specific research activities and working group meetings with leading legal scholars, attorney practitioners, and industry thought leaders, the group is examining the following questions:

- Whether a market failure exists, and if so what is the precise nature of this failure in the cyber security area?
- What legal and institutional impediments exist for developing decentralized solutions to the cyber security problem?
- What strategies exist for removing these impediments?
- What regulatory and legislative changes are necessary to support decentralized solutions?

Dean and Professor of Law Mark F. Grady holds an A.B. (1970) Summa Cum Laude in Economics and a J.D. (1973) from UCLA.

Some key considerations for protecting critical infrastructure, and uncovering potential market concerns, include:

- 85 - 90% of critical infrastructure assets (e.g., power grids, financial systems, communications systems) are owned by civilians, and assets can be disabled by an attack that disables their computer controllers;
- Systems have multiple owners whose computers are interconnected;
- Malicious actors can exploit the weakest link on the network computer;
-- Individual asset owner investments in computer security are borne by asset owners but benefits are spread throughout the network. Information useful in defending a network against attack (e.g., an intrusion fingerprint) can be competitively damaging to the network member that might share this information with other members (e.g., a bank might be reluctant to reveal to its competitors that its accounts have been looted).

CIP Project Fellow and Visiting Assistant Professor Amitai Aviram was educated at Tel-Aviv University School of Law (LL.B., 1995) and at the University of Chicago Law School (LL.M., 2000).

Some of the decentralized solutions being evaluated as potentially more effective and efficient methods of providing for cyber security include;

- Security cooperatives. Network members (e.g., banks or electric power companies) organized into security coops establishing cyber security standards for members. These standards may differ according to the cost circumstances of each member and enforcement of these standards would be accomplished privately through expulsion, penalties, forfeiture of performance bonds, and so forth.
- Contracts. Network members contracting with each other for reciprocal undertakings of precaution responsibility. This process would be connected to the process by which the members grant access rights to each other.
- Insurance loss prevention. First-party or third-party insurance for cyber losses providing for a means to establish and enforce cyber security standards. Impediments to insurance include (1) the lack of actuarial data; (2) the difficulty of insuring the correlated losses that could arise from a cyber attack.
- Civil liability. Exploring feasibility of tort law liability in cases of computer owners negligently allowing malicious actors use of computers to harm others.

Attacker Fingerprinting and Identification
Led by Sushil Jajodia

The purpose of this project is to develop techniques to identify attackers based on their attack fingerprints. This project will concentrate heavily on the use of data mining for two reasons. First, the volume of data dealing with both network and host activity is so large that it makes it an ideal candidate for using data mining techniques. Second, data mining has been applied successfully for effectively implementing tools to detect and analyze intrusions.

The project will consist of three phases:

1. Fingerprinting phase learns signatures and builds profiles of specific attackers (insiders, known hackers, nation states) by mining security information sources, e.g., host logs.

Sushil Jajodia is BDM International Professor of Information and Software Engineering and Director of the Center for Secure Information Systems at GMU. Dr. Jajodia received his Ph.D. from the University of Oregon.

2. Analysis phase will extract and deduce information such as overall attack strategy, specific techniques/tools applied, sequences of techniques, and level of aggression.

3. Identification phase applies fingerprinting rules to new attack data.

The goal of this research is not just to identify an attacker, but also to measure the effects of the attack.

Internet Infrastructure Project
Led by Laurie Schintler and Sean Gorman

The events of 9/11 brought a new focus to the vulnerability of the US economy to attack from malevolent forces. The dependence of the new economy on information has made the infrastructures that supply it critical to the functioning and stability of the nation. The Internet and IT depend on physical fiber to connect the various computers, servers, switches and routers that provide the underpinnings of the US information infrastructure that are all vulnerable to attack. This study will attempt to gain a better understanding of the topology and structure of our nation's complex telecommunications infrastructure. The analysis will be formed at a national level (macro-level) and a city-level (meso/micro-level) involving several key metropolitan centers.

Laurie Schintler is an Assistant Professor of Public Policy. She received her Ph.D. at the University of Illinois at Urbana-Champaign, 1995.

From a macro-level perspective, the study will identify what cities are most "critical" to the telecommunications network, playing a pivotal role in receiving and disseminating information via the Internet. The study will examine how the connectivity and performance of the Internet would be affected by the removal of "critical" cities from the network resulting from a physical attack on some key infrastructure facilities. The micro-level analysis will examine the spatial distribution of information infrastructure in several central locales and how this infrastructure interfaces with banking and financial institutions and the services they provide. Critical nodes in these cities will be identified.

The findings of this analysis will be used to derive a set of policy and planning recommendations on how best to mitigate the catastrophic and cascading effects that could occur as the result of a targeted physical and/or cyber attack on the nation's telecommunications infrastructure.

High Reliability Networks, Disaster Mitigation and the World Trade Center: Analysis of Technological, Organizational and Social Factors Affecting Performance of a Critical National Economic Concentration

This research program aims to "drill down" to exploit specific case material arising from the World Trade Center (WTC) event of September 11th. It will provide detailed data to inform policy thinking presently focused largely on the conceptual level. It will build on the role of national authority in re-establishing key crashed networks. The research will cast its findings in terms of the existing scientific literature on emergency management. It will focus on the technological, organizational and human factors making up this economic concentration.

Sara Cobb, Director of the Institute for Conflict Analysis and Resolution, holds a Ph.D. in Communication from the University of Massachusetts - Amherst, 1988

Arthur Melmed is a Research Professor at the GMU School of Public Policy. He is a graduate of the City College of New York and Columbia University in electrical engineering and computer science

Todd La Porte is a Research Associate Professor at the GMU School of Public Policy. La Porte received his Ph.D. in Political Science from Yale University in 1989.

Carlos Sluzki, MD, is a Research Professor at the GMU School of Public Policy and the Institute for Conflict Analysis and Resolution. Dr. Sluzki was educated at the University of Buenos Aires School of Medicine.

The activity aims to capture what happened to critical infrastructures in Lower Manhattan and the region on which it draws: (1) on September 11th; (2) during the days and weeks following the attack; and (3) at the one year anniversary. The study will focus primarily on the reestablishment of the financial markets on Wall Street and the systems necessary to get them up and running.

Analytic descriptions will be assembled using standard documentary research methods, subjected to appropriate content analysis techniques in order to ensure consistency in organizational analysis. Documentary data will be supplemented with selective interviewing of key players using a "snowball" research technique, necessary where high levels of trust are required to access sensitive information, and where key respondents are not known prior to the start of interviewing.

Results will be assembled in a form useful to high-level policy and decision-makers, public and private.

A Comparative Analysis of Technological, Organizational and Human Factors Affecting Security in a Civilian and Military Network-Dependent Infrastructure Cluster: Crystal City and the Washington Navy Yard

This research program aims to examine, classify and analyze the differing dependencies for continued operation and disaster recovery of network-dependent infrastructure in a civilian and military concentration, including technological, organizational, jurisdictional and human factors. The concentrations selected are Crystal City, VA and the Washington Navy Yard in the District for which much of the required data are available through the office of the Department of Navy Chief Information Officer by a Memo of Understanding with George Mason University.

The military has the design goal for network-dependent infrastructures, say an aircraft carrier or, in this case, the Washington Navy Yard, of maintaining operational performance in the circumstance of a destructive event. The military is a high-reliability organization.

The civilian market place has the economic "design" goal of maximizing efficiency and reducing costs, leading to network-dependent economic clusters like Crystal City. In the circumstance of a destructive event, the economic goal gives way nearly instantaneously to the political and social goal of the evacuation and safety of the largest number of civilian workers.

For a high-reliability organization, vulnerability to a destructive event means graceful degradation, i.e., continuing to maintain a measure of effectiveness in the circumstance of a destructive event, with the contingent potential for relatively rapid recovery of full performance. For a civilian infrastructure cluster, vulnerability to a destructive event implies a phase change in goal, with the contingent potential of a long delay in recovery of lost economic performance. (*continued, page 9*)

(*Project Highlights, continued from page 8*) For the U.S., unscathed at home by overseas opponents since the war of 1812, this distinction between military and civilian vulnerability may not survive the threat and actuality of domestic terrorism. This study aims to assess and assemble comparative vulnerability factors in a form useful to high-level policy and decision-makers, public and private.

The results will be presented for consideration and use by government officials and industry representatives at a conference in the Washington metropolitan area scheduled for Fall 2003.

Drs. Cobb, Melmed, LaPorte, and Sluzki are working jointly on the WTC and the Crystal City / Navy Yard projects.

Network Security Risk Assessment Model and Portable Network Security Analysis Tool
Led by George Baker, Taz Daughtrey, and Malcolm Lane

The JMU CIP Research and Support Center includes research specialists from the College of Integrated Science and Technology and the Nelson Institute of James Madison University. This Center will provide technical expertise for three major CIP activities:

1) The design of the *Network Security Risk Assessment Model* (NSRAM)
2) The development of the *Network Security Risk Assessment Modeling Tool* (NSRAMT) that incorporates NSRAM
3) The design and development of the *Portable Network Security Analysis Tool* (PNSAT)

The data produced by PNSAT will provide the necessary inputs for NSRAMT. Both tools are required for developing and supporting policies and regulations related to Cyber Security.

Faculty and graduate student researchers in the Integrated Science and Technology Department will be responsible for NSRAM (the model). Faculty and student researchers and developers in the Department of Computer Science (some affiliated with the Commonwealth Information Security Center) will be responsible for the development of the modeling tool NSRAMT and for the design and development of PNSAT. JMU policy specialists will also participate with George Mason University (GMU) researchers in CIP policy activities.

Dr. George Baker is the Interim Director for the Institute of Infrastructure and Information Assurance. He holds a Ph.D. from the U.S. Air Force Institute of Technology.

Taz Daughtry works in Computer Science at JMU. He holds an MEd from the University of Virginia in Science Education.

Dr. Mal Lane is the Department Head of Computer Science at JMU. He holds a Ph.D. from Duke University.

Dr. Lloyd J. Griffiths, Dean of the School of Information Technology and Engineering, GMU

"Securing the networks supporting the nation's critical infrastructures involves more than purely technical solutions. In fact, securing these systems involves the rather interesting and challenging intersection of law, public policy, and information technology."

Dr. A. Jerry Benson, Dean of the College of Integrated Science and Technology, JMU

"Along with developing a risk assessment model to help secure our critical infrastructures, research is being conducted at James Madison University through the Commonwealth Information Security Center. These projects allow us a unique opportunity to combine the efforts of our researchers to solve security issues at the state and national levels."

CIP WHITE PAPER:
Understanding the Implications of Interdependencies and Cascade Effects with Respect to Infrastructure Protection

by Kip Thomas, Ph.D. Candidate
Research Associate Professor, School of Public Policy, George Mason University

Tragic terrorist actions, like the Oklahoma City bombing, Kobar Towers, the attacks on the World Trade Center and Pentagon, and the disruption of the U.S. Postal Service with the anthrax attacks has widened recognition of the fragility of modern infrastructures. This heightened awareness has resulted in a sense of urgency and pressing need to develop systems and methods of operation that provide greater infrastructure security, resiliency, capacity, and preparation for times of crises. The term "critical infrastructure" has emerged as a method of identifying and classifying key infrastructures, defined as "a network of independent, mostly privately-owned, man-made systems and processes that function collaboratively and synergistically to produce and distribute a continuous flow of essential goods and services."[1]

While this definition is accurate, it may in fact impose self-limiting constructs on emerging methods of risk identification, preparedness and mitigation strategies. These limitations stem from a failure to recognize the interdependency of modern infrastructures.

Infrastructure protection requires a myriad of organizations, institutions and agencies to come together in methods, practices, standards, regulations, and policies that protect individual and system-wide interests, both physical and virtual, now and in the future. This is no easy endeavor when considering that methods must be developed for reliable and consistent information and infrastructure protection (e.g., information management and sharing, standards, and practices) while protecting sensitive business and governmental interest at all levels.

Complicating this issue is the reality that policies and procedures designed through economic and policy incentives to provide infrastructure protection must be crafted in such a way as to create public goods that favorably contribute to overall national security, without limiting productivity, innovation or enterprise. In addition, technological innovation and obsolescence greatly affect the criticality of particular infrastructures. Further, technological innovation occurs through not only scientific advancement but is influenced "through both market and non-market transactions and that the latter involve not only business but also public organizations that exercise considerable influence over broader institutions (e.g., regulatory regimes.)"[2]

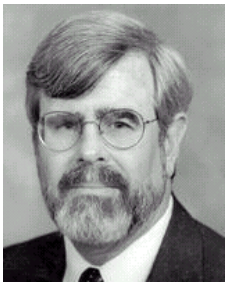
It is important however, to recognize that while the infrastructure protection problem is difficult, much has and is being done to address these concerns. Beginning with the recognition of the need for homeland defense in the U.S. Constitution and the establishment of the National Guard there has been a clear understanding of the need for homeland protection. In response to the significant technological advances and threats imposed from the atomic bomb, the Civil Defense Act of 1950 was enacted as "the policy and intent of Congress to provide a system of civil defense for the protection of life and property in the United States from attack and from natural disasters."[3]

Understanding the complexity of risks imposed from the threat of attack and natural disaster, the concept of Comprehensive Emergency Management (CEM) emerged as a process to manage their consequences. The four phases of the CEM process include mitigation, preparedness, response, and recovery.

> *MITIGATION* activities actually eliminate or reduce the chance of occurrence or the effects of a disaster (e.g., requiring protective construction materials to reinforce a roof to reduce damage from a hurricane).
> *RESPONSE* activities occur during and immediately following a disaster providing emergency assistance to victims of the event and reducing the likelihood of secondary damage.
> *PREPAREDNESS* is planning how to respond in case an emergency or disaster

(*continued, page 11*)

John Burke, General Counsel, BITS



"On behalf of my clients, I am excited to be a part of GMU's CIP efforts exploring legal and policy issues for critical infrastructure use and protection."

Phil LaCombe, Senior Vice President and President, Security & Protection, Veridian

"The CIP Project at GMU presents a unique opportunity to examine evolving technical challenges in the field of CIP. Veridian looks forward to collaborating with the CIP Project and the experts affiliated with it."

John W. Thompson, Chairman and CEO, Symantec Corporation

"With more than 85 percent of the nation's critical infrastructure owned and operated by private entities, public/private cooperation is critical to securing our nation's virtual borders."

(*White Paper, continued from page 10*) occurs and working to increase resources available to respond effectively.

RECOVERY continues until all systems return to normal, or near normal. Short-term returns vital systems to minimum operating standards. Long-term restores systems, hopefully less disaster-prone.

This CEM approach was institutionalized in 1979 with the creation of the Federal Emergency Management Agency (FEMA). "FEMA resulted from the consolidation of five federal agencies that were dealing with many types of emergencies"[4] including the Federal Insurance Administration, the National Fire Prevention and Control Administration, the National Weather Service Community Preparedness Program, the Federal Preparedness Agency of the General Services Administration and the Federal Disaster Assistance Administration activities from HUD. Civil defense responsibilities were also transferred to the new agency from the Defense Department's Defense Civil Preparedness Agency. Since that time, many state and local organizations have accepted this approach and changed the names of their organizations to include the words 'emergency management.'[5]

Recently, FEMA has coordinated its activities with the newly formed Office of Homeland Security, and FEMA's Office of National Preparedness has been given the responsibility for helping to ensure that the nation's first responders are trained and equipped to deal with weapons of mass destruction. Billions of dollars of new funding have been directed to FEMA to help communities face the threat of terrorism. Just a few years past its 20th anniversary, FEMA is actively directing its "all-hazards" approach to disasters toward homeland security issues.

The burden of disaster management requires a close partnership among all levels of government (Federal, regional, state, county, and local) and the private sector (business and industry, non-profit organizations, and the general public). In recognition of the realities of the many players necessary in emergency management, the CEM process has been amplified by FEMA to include a more comprehensive and integrated approach termed Integrated Emergency Management System. This process, based on CEM principles, includes the specific goals of:

- fostering full federal, state and local government partnerships with provisions for flexibility at the several levels of government for achieving common national goals;
- emphasizing implementation of emergency management measures which are known to be effective; and,
- achieving more complete integration of emergency management planning into mainstream state and local policy making.

Additionally, significant analysis and effort has been devoted to the identification of threats to infrastructures based on geopolitical conditions, and in proposing possible government organizational changes to provide for enhanced security. One key source for this work is the United States Commission (*continued, page 12)*

Dan Porter, Department of the Navy, Chief Information Officer / Critical Information Assurance Officer

"The DON CIAO is responsible for developing a plan for protecting the Department's critical cyber and physical infrastructure and to coordinate remediation efforts. Ultimately, DON CIP strives to be integrated into, and become a major contributor to, a national CIP protective network that optimizes the positive power of the federal sector to protect the citizenry, institutions, and continuity of government operations."

Margaret Purdy, Associate Deputy Minister, Department Of National Defence, Ottawa, Canada, Office of Critical Infrastructure Protection and Emergency Preparedness

"The relationship between research and security has been too little explored and too often overlooked, in my view. It is a relationship that is crucial not only to those of us directly involved in either research or security, but to all of us as citizens in an increasingly complex and hazardous world."

(*White Paper, continued from page 11*) on National Security/ 21st Century, Seeking a National Strategy, commonly referred to as the Hart-Rudman Commission. This commission's final report, completed in February 2001, accurately identified the possibility of tragic occurrences such as that of September 11, 2001.

The Hart-Rudman Commission's recommendations for governmental response to Homeland Security (a key component and enabler of CIP) have received bipartisan support and have been largely adopted by the administration, congress, and the judiciary. Central to the Commission's recommendations to address Homeland Security (and actual government actions taken to date), has been the creation of a Homeland Security organization based on the Federal Emergency Management Agency structure. This new organization acts as a central coordinating point for homeland security. This is in keeping with the Hart-Rudman Commission's recommendation that this activity be charged "to consolidate and refine the missions of the nearly two dozen disparate departments and agencies that have a role in U.S. homeland security today." However, the establishment of the Office of Homeland Security in the White House and not as the Commission's proposed National Homeland Security Agency (NHSA) may impose future regulatory, budgetary, and policy implications and may limit the development of effective cooperative policy structures with industry and interested parties. Both the House and Senate have recognized these potential problems and current legislation is pending to establish the NHSA.

The efforts thus far discussed reflect the complexity of protecting the nation's critical infrastructure, but they have focused only on government initiatives. Developing a deeper understanding and appreciation of the intricate relationships between government, industry, and interest groups involved in infrastructure protection and homeland security is vital to the success of infrastructure protection policy and management.

While recognizing the four-phase approach developed and implemented by the CEM process and FEMA, practical processes and methods of collaboration between government, industry, and interest activities in determining future security and capacity requirements must be pursued (e.g., policy coordination and measurement and analysis methods). This requires development of more cooperative and collaborative policy, regulations, and standard-setting arrangements and greater effectiveness of government, industry, and interest activity relationships.

The emergence of cooperative industry initiatives in developing standards provides examples of viable coalition activities, or cooperative policy structures. In fact, it appears that collaborative networks may have become the dominant sociological means of achieving consensus for standards and plans of action. Nonetheless, network collaboration has been met with cumbersome regulatory and statutory burdens in the United States in finding acceptable means of action.[6]
(*continued, page 13)*

(*White Paper, continued from page 12*) The existence of self-organizing collaborative industry activities does not mean that future regulatory policy will be solely abrogated to the market. In fact, it requires the resurgence of regulatory policies that afford general rules and more involvement in developing future outcomes.

[1] Critical Foundations: Protecting America's Infrastructures, the report of the President's Commission on Critical Infrastructure Protection (PCCIP) 1997
[2] Rycroft, Robert W. and Kash, Don E., The Complexity Challenge: Technological Innovation for the 21st Century, A Cassel Imprint, Wellington House, New York, NY 1999, pg. 218
[3] United States Commission on National Security/21st Century, *Road Map for National Security: Imperative for Change*, Jan 31, 2001
[4] THE EMERGENCY PROGRAM MANAGER, Federal Emergency Management Agency Emergency Management Institute, http://training.fema.gov/EMIWeb/is1.htm downloaded Mar 28, 2002
[5] http://www.fema.gov/about/history.htm downloaded 30 March 2002
[6] Rycroft, Robert W. and Kash, Don E., pgs. 81-83, 103, 130

CIP Scholar Assessment of Recent Attack on Internet Root Servers

by Professor Laurie Schintler

"The heart of the Internet sustained its largest and most sophisticated attack ever, starting late Monday, Oct. 21, 2002, according to officials at key online backbone organizations. Around 5:00 p.m. EDT, a "distributed denial of service" (DDOS) attack struck the 13 "root servers" that provide the primary roadmap for almost all Internet communications. Despite the scale of the attack, which lasted about an hour, Internet users worldwide were largely unaffected, experts said." ("Attack On Internet Called Largest Ever" by David McGuire and Brian Krebs, washingtonpost.com Staff Writers Tuesday, October 22, 2002)

While the attack on Monday of key root servers was one of the largest recorded in the history of the Internet, it occurred only for a short duration and was limited only to Domain Name Root servers. Said Sushil Jajodia, Director of the Center for Secure Information Systems at GMU, "The good news is that the attack was unsophisticated and awkward. It is not clear what the objective of the attack was. If the objective of the attack was simply to disable DNS, the attackers were only mildly successful and that only for a short period of time. The bad news is that the current IP-based infrastructure is inherently weak and will provide a lot of opportunities for future attacks well into the future. If the attackers had been more sophisticated, the attacks could have been more effective at disrupting DNS, lasted longer, been harder to track down, and been harder to mitigate. The fact that this could have been executed by a single teenager speaks volumes about the state of the information infrastructure."

"(This attack) didn't impact the Internet much, because the Internet is resilient and operators were quick to respond," said Tiffany Olsen, spokeswoman for the President's Critical Infrastructure Protection Board, the group responsible for creating the United States' National Strategy to Secure Cyberspace. However, there "will be larger attacks than this one was." ("Net attack--how it was squashed" by Robert Lemos, Special to ZDNet News, October 23, 2002).

The average user did not experience any problems because most of the hosts were able to resolve the IP/Domain name using their local Domain server and cache memory that resides on these servers. In other words, host servers were able to get service without having to access the root servers. In fact, DNS clients need to communicate with root servers only occasionally, on average eight times a week, according to one network engineer. Also, the attack resulted in no more than 100m/bits of traffic, a fairly low volume by DDOS standards. And of course, there is a question of whether or not enough root servers were shut down – some engineers have suggested that at least eight root servers would have to be taken down before any serious problems could arise. One cautionary note is that this most recent attack seems to suggest that cyber-criminals are getting more sophisticated, targeting key infrastructure pieces in a systematic manner. It would be safe to assume that they are progressing their learning curve quickly, and security measures need to stay ahead of attackers' ability to cause damage.

Institute for Infrastructure and Information Assurance at James Madison University

James Madison University recently announced the creation of the Institute for Infrastructure and Information Assurance (I^3A). Infrastructure assurance is high on the national agenda. However, the lack of coordination among several well intentioned but splintered efforts and agencies is an apparent weakness in meeting this challenge. At James Madison University, conversations with federal and state officials reinforce the need for a coordinated effort that "connects the dots" by looking broadly at the infrastructure assurance problem.

The broad set of activities comprising infrastructure assurance embrace both information security and physical security; federal, state and local activities; and government and private industry organizations, and will require multidisciplinary solutions including science, technology, social science, and public policy.

The Institute for Infrastructure and Information Assurance (I^3A) was established to provide the integrative force needed to encompass and coordinate several university efforts including the CIP Project and the Commonwealth Information Security Center (CISC) activities. The CISC at JMU is currently studying issues in secure mobile commerce, secure groupware, information security policy impersonation, and specification of trusted systems.

CIP Project Staff

Kevin "Kip" Thomas
Research Associate Professor / Working Groups Project Manager

Meredith Gilchrest
CIP Law and Policy Research Archivist/ Outreach Program Manager

Rebecca Luria
CIP Project Administrator / Executive Assistant

George Baker
Interim Director JMU Institute for Infrastructure and Information Assurance

Ken Newbold
JMU Outreach Coordinator / JMU CIP Project Liaison

Contact: cipp01@gmu.edu
703-993-4840

The mission of the institute is to facilitate development, coordination, integration, and funding of activities and capabilities of the James Madison University academic community to enhance information and critical infrastructure assurance at the national, state and local levels. The I^3A will leverage current grant activities and products and related university programs to address the broader infrastructure assurance challenge.

The Institute for Infrastructure and Information Assurance is under the direction of Dr. George Baker. For further information, please contact Dr. Baker at (540) 828-8767 or bakergh@jmu.edu.

Frank Sesno, CIP Fellow

Few people in broadcast journalism have had Frank Sesno's breadth of experience or his range of access, reporting and decision-making. During 17 years at CNN, Sesno held a unique progression of influential, high profile positions, culminating in his elevation to senior vice president and Bureau chief in Washington, where he was responsible for the largest news gathering operation at CNN - including its White House, Congressional, Pentagon, National Security, and political reporting. Sesno has served as CNN's White House correspondent, appeared frequently on Inside Politics and hosted Newsday and Late Edition. Currently, Sesno develops mini-series for The History Channel, including one on the life of Ronald Reagan, and is professor of public policy and communication at George Mason University, with whom he is developing a weekly program to air on PBS. With signature wit, he offers an intriguing perspective on how changes in politics, technology and the media will affect an ever-shrinking world.

NSA Director to Speak at GMU on Nov. 12

On Tuesday, November 12, at 6:30pm, you have the opportunity to participate in a unique event—a question-and-answer forum with America's chief eavesdropper, who now finds himself and his agency on the frontlines of America's war on terrorism. Lieutenant General Mike Hayden, Director of the National Security Agency, has agreed to a highly unusual public forum as a guest of University Professor Frank Sesno. The event, sponsored by the CIP Project, is to be introduced by George Mason University President Alan Merten. It will take place in Dewberry Hall.

Hayden will address issues ranging from the delicate balance between personal privacy and national security in the current context to the challenges involved in preventing a second 9/11. He will discuss his recent Congressional testimony and the circumstances surrounding the now-famous September 10, 2001 intercept and the challenges of changing a Cold War spy organization into a 21st century intelligence agency facing asymmetrical warfare. General Hayden will discuss the consequences of media leaks and how we strike a balance between necessary secrecy and an informed public.

In addition to his service as the Director of the National Security Agency, General Hayden has served in a number of command and staff positions in a career that spans 35 years. Highlights include time spent on the National Security Council staff, as well as command of the Air Force Intelligence Agency.

Come hear the nation's foremost authority on signals intelligence address these and other issues in "A Conversation with the NSA Director: Eavesdropping on Osama bin Ladan—can we prevent the next 9/11?

The CIP Report is published by LegalNet Works, Inc. on behalf of the CIP Project. Formed in 1996, LegalNet Works Incorporated focuses on the development of information security laws and regulations with an emphasis on liability, risk management, national security, regulatory compliance, and privacy. LegalNet consults both government and industry officials on legal and policy reform in these complex areas.

If you would like to be added to the distribution list for *The CIP Report,* please send an e-mail to cipp01@gmu.edu.