JULY 2003 / VOLUME 2, NUMBER 1

THE CIP REPORT

CIP PROJECT STAFF

John McCarthy, *Executive Director*

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

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

Rebecca Luria, *CIP Project Administrator / Executive Assistant*

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

George Baker, *Associate 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.

This edition of The CIP Report is dedicated to the important contribution that academia provides in vital research which gives us the opportunity to uncover some of the more difficult challenges we face in providing for national security, economic well being, public health and maintaining public confidence. We are honored to have a message from the former Attorney General Edwin Meese, a distinguished fellow and holder of the Ronald Reagan Chair in Public Policy at the Heritage Foundation, and Rector of George Mason University. His message relates to how academic institutions can address national security concerns through responsible involvement of government and industry in the research process.

Through academic research, we are able to raise awareness and work towards practical solutions. In addressing these concerns, however, scholarly research benefits greatly through collaborative actions between government, industry, and academia.

We at the CIP Project have encouraged this type 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 Protection of Key Assets and the National Strategy for Cyber Space Security. The intersection of maintaining academic freedom and preserving national security is the challenge we presently face, but we know that through responsible information sharing we can achieve what is in our best interest as scholars and as a nation. Many of you have probably seen the media attention concerning the Internet Infrastructure Study project involving Professor Laurie Schintler and Sean Gorman, a doctoral candidate in the School of Public Policy. We have included an article in this edition of The CIP Report that discusses how this activity has allowed GMU to further the debate and development of methods for public and private cooperation with academia.

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

Another effort of the CIP Project in support of information sharing is the series of CIP Critical Conversations being moderated by CIP Project Scholar and GMU Professor of Public Policy, Frank Sesno. We had our first Critical Conversation entitled: "Protecting America's Critical Infrastructures: From the War Room to the Board Room" on June 18th, 2003 at the National Press Club. 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. We have included excerpts from the transcript in this edition, for a complete copy of the transcript you can visit our website at: http://techcenter.gmu.edu.

Academic Freedom and Scientific Research in a Vulnerable World

By Kip Thomas and Ami Carpenter

The question of how to balance the limitations imposed by national security concerns with the openness required for innovative and cutting edge academic research has been a keen topic of discussion and debate since the September 11th tragedy. As one example, in March of this year the Potomac Institute sponsored "The Role of the Post-September 11th Intersection of Security Constraints and the Need For Open Scientific Research", a forum which focused on the impact for traditionally open research environments by post 9/11 security guidelines from Congress, Department of Defense, and the Department of Homeland Security. The forum included discussion of foreign nationals studying in the United States and the study of "sensitive, but unclassified" material.

As noted during this event, one unfortunate outcome of this heightened security concern is that an environment of secrecy is developing. Already, the post 9/11 atmosphere poses serious challenges to openness and innovation as previously available open source data have been removed from the Internet and other outlets. Since these potential restrictions and hindrances to basic research are occurring at the same time that the country is looking for technological innovation to solve problems, it is currently of critical value to reconcile the openness of information and knowledge necessary for scientific research with heightened national security concerns.

In previous efforts to address this concern, the Reagan administration issued executive order NSDD189, which states that no restrictions may be placed on fundamental research, with the exception of that work that affects national security. Additionally, the President's National Strategy to Secure Cyberspace discusses a broad framework with regard to cooperation with industry, government, and academia. While these attempts at providing guidance

(Continued on Page 3)

A Message from Former Attorney General Edwin Meese

Freedom of information has always been a source of vital concern for our nation. So much so, that the First Amendment to our Constitution is dedicated to the very values and principles of free speech. This freedom brings with it the responsibility to be appropriate and honest in statements that are made by individuals or by researchers in their efforts to advance a body of knowledge. This does not mean that we should limit our innovations nor should we limit our research and development communities. We need to continue to press on with innovations and new technologies that will provide better security while still allowing for the freedom provided in the First Amendment. Having said this, it is important that we recognize that national security needs require certain protections to ensure that vulnerability information, or information that may be useful by individuals for nefarious purposes, is denied to those who would abuse it.

I believe that George Mason University has begun this process. The Critical Infrastructure Protection Project is involved with government, industry and other academic institutions to insure that the information generated by their research activities has appropriate coordination to identify and protect sensitive information. This identification allows the research to continue, yet identifies those items that should be kept private. In addition, such identification places a responsibility on those who must provide for enhanced security. This feedback is invaluable in developing new security practices for both government and industry. This is truly a situation where academia has become a partner with government and industry to enhance our nation's security.

Edwin Meese III
Rector
George Mason University

Academic Freedom *(Continued from Page 2)* have been helpful, there remains a lack of understanding in how to accomplish the objective of allowing academic freedom while providing for national security objectives.

Kip Thomas

Of key importance is the clarification of certain terms which currently serve as conceptual guides for policy makers, particularly the term sensitive but unclassified. Ambiguously defined terms such as this one offer flexibility of interpretation, but invoke a series of questions related to how issues and actions are framed and acted upon. What is the disparity between how academic institutions and government agencies interpret this term? By whose criteria are definitions legitimized? Who defines 'sensitive' and 'unclassified'? These questions are important because framing policy issues tends to frame approaches to addressing them, and therefore outcomes as well. Thus the question of primary importance is how collaborative relationships between government agencies and research institutions can be established to explore different perspectives on freedom of information, with the common concern of national security.

A process for government agencies, industry and academic institutions to work together, where respective objectives can be jointly created and agreed upon through clear policy guidelines is lacking. One near term method of action is for universities to outreach with responsible private sector and government organizations to manage research information.

The CIP project has uniquely positioned itself to play an important coordinating function and begun the process of developing methods for a longer term collaborative model. George Mason University and the CIP Project have served as a gathering place for leaders in the Homeland Security and critical infrastructure protection space, filling a void that has been growing as various initiatives are launched without cooperation across the board.

Ami Carpenter

Leaders in the critical infrastructure protection communities are the CIP Project's primary constituencies. A unique aspect of the CIP Project is that it has purposefully brought together highly qualified and knowledgeable experts with significant experience in cyber security and critical infrastructure protection from government, the public and private sectors, along with renowned academic scholars from an interdisciplinary and multi-institutional perspective to carefully and deliberately address and develop solutions for these areas of pressing national security. This deliberate inclusion of a multiplicity of relevant actors gives the CIP project the credibility to convene forums for collaborative dialogues between public and private institutions, where issues in conflict between public and private sectors can be jointly addressed. ❖

Protecting America's Critical Infrastructure: From War Room to Boardroom

On June 18th, the Critical Infrastructure Protection (CIP) Project hosted "Protecting America's Critical Infrastructures: From War Room to Board Room," the first in a series of "CIP Project Critical Conversations." Endeavoring to bring together government and industry leaders, legislators, and scholars to discuss key issues and inform about the progress toward preparedness, the status of information and awareness, and the actions that we can all take to make our nation a safer place to live, this first Critical Conversation centered on the controversial debate over the roles of government and industry in shouldering the costs, setting priorities and bearing responsibility for the protection of America's critical infrastructure.

The event brought together five of today's leading policymakers, government officials, and corporate executives to offer unique, first-hand insight into U.S. homeland vulnerabilities, defense preparedness and technological strengths and weaknesses, and to debate the delicate balance of responsibility and information sharing that is necessary between government and industry to effectively implement critical homeland security initiatives.

After opening introductions by John McCarthy, Frank Sesno, moderator of the event and GMU Professor of Public Policy and Communication and Senior Fellow of the Critical Infrastructure Protection Project, engaged the panel members, asking each to comment on their priorities for making critical infrastructure safer in the year ahead.

Cable Risdon Photography

Asa Hutchinson, Under Secretary for Border and Transportation Security with the Department of Homeland Security: Under Secretary Hutchinson noted "the significant amount of progress for the first steps of critical infrastructure protection." He outlined his priorities as, "Partnerships, intelligence sharing assessments, knowing where we're going, pilot projects, those are our priorities." He also stressed the importance of partnerships: "From a government standpoint, I think strict regulation is probably the last resort. And so our emphasis should be on building the support in the private sector, building that cooperation, increasing pilot projects with them when we have funding from Congress. I think those are all an important part of the strategy and the priorities that we should engage in."

Congressman Jim Turner, U.S. Representative (D - TX), Chairman House Select Committee on Homeland Security: From Congressman Turner's perspective on the Homeland Security Committee, his top priority is actually the process of setting priorities, "and then [having] the courage and commitment to address those first." Congressman Turner views the recent legislation as two groups of items, "One is the massive merger of 22 agencies for the primary purposes of giving those agencies a new direction and a new sense of what they're about which is to protect the security of the American people. The other group of items in that bill, what I call the new things, the things we weren't doing before. From my perspective, the important thing for us to accomplish in the shorter term is to make the new things that were in that legislation work."

Cable Risdon Photography

Honorable John Hager, Assistant to the Governor of Virginia for Commonwealth Preparedness: Mr. Hager stated that "As the paradigm has shifted in homeland security to one of prevention and vulnerability reduction, I think it's very timely

(Continued on Page 5)

Cable Risdon Photography

Critical Conversation *(Cont. from Page 4)* that we talk about critical infrastructure, because that's where the action is. And in fact, that's what we owe to our citizens for their safety and security." "Why focus on critical infrastructure? Number one, we owe it to our citizens. Number two, it is the total economic backbone of the Commonwealth and the income to the state. And how we handle it will determine our future from an economic development standpoint as we go down the road." At the state level, "we tend to be very action oriented."

Ms. Catherine Allen, Chief Executive Officer of BITS, the Technology Group for the Financial Services Roundtable:

Cable Risdon Photography

"What I believe terrorists would like to do is undermine public confidence and really shut down our economy. And that could occur if, in fact, major financial institutions and payments and settlements infrastructure were effected. Because of that, we focus very much on cyber security and the concerns about making sure that the electronic systems have redundancy and are up and running. We also pay attention to things like communications. The ability to get our CEOs, the Department of Treasury, DHS and other groups to be able to talk if there is an incident because it's as much about ensuring public confidence as it is about fixing those systems in the back rooms. We're also concerned about interdependencies. Lastly, it's very important that we share information. That we have the ability, with some protections from both anti-trust and FOIA, to be able to share with each other the valuable data about what is happening in our institutions."

Mr. John Derrick, Chairman of the Board and former CEO of Pepco Holdings, Incorporated:

Cable Risdon Photography

"What I'd like to see a year from now is a lot of answers, and a lot of action on some of the things that have been touched on here. I would say there are three overarching questions that we're all engaged with here. One, what should be done? Two, who pays? And three, who decides the first two? I think a year from now it's very safe to say, we'll be more ready. But what ready means is something that I think we need to spend a fair amount of time working together on."

Following opening remarks, the panelists engaged in a discussion about various topics related to critical infrastructure protection and homeland security.

Priorities for DHS

Hutchinson: "We've got work to do, but I think that we have the right strategy. And we hope that one year from now that strategy will be way down the line in terms of implementation."

Turner: "But I also believe that the responsibility that was given to the department in this area of collecting intelligence information in a central place, and matching that up with a fair and clear analysis of our vulnerabilities, is the key to making the Department work. And the Office of Information Analysis is in many ways the nerve center of the Department. It not only has to function in order for the rest of the agencies to know what they're to do on a daily basis, and what their function is, but at some point, it is also clear that this information has got to flow down to the states and the localities. Because one of the things you hear most commonly from local officials, law enforcement, mayors, is 'what's this alert about and what am I supposed to get ready for?' So I think that issue is one that should be dealt with, but I think it's also symbolic of the problem that I mentioned. And that is, we are in a stage right now where we're saying we've got to get ready for everything and everybody's got to do everything."

Balancing Regulation and Security - Roles and Responsibility

Turner: "There's certainly a great risk of over regulation here. But, the bottom line is that these decisions can't be made by one

(Continued on Page 6)

Critical Conversation *(Cont. from Page 5)* congressman. They can't be made by Congress as a whole. The right place to make these decisions is through the Department of Homeland Security that I think was charged by the Congress in the Homeland Security Act to carry it out."

Hager: "We talk a lot about shared responsibility when we get to critical infrastructure. But I think equally important as shared responsibility is defined roles. We have certain roles at the state level. One role is to work with our universities in this benchmark, such as the George Mason project on critical infrastructure, which is designed to define the roles of local, state, federal, government and the private sector across the 13 critical infrastructure sectors. Particularly here in the national capital region, we're trying to make this region a model, if you will, for the country. I think that project is going to go a long way in helping to define the roles of the players here. Because so often, those roles muddy and cross over. So role definition, and intelligence is a good example of that, comes from all sources. But you've got to bring it together and fuse it, and then turn it back around rapidly so that it can be used by the people on the ground at the state and local level who really need it and who can do something with it."

John McCarthy and Frank Sesno confer with Dean Lloyd Griffiths from GMU prior to panel commencement.

Public/Private Incentives

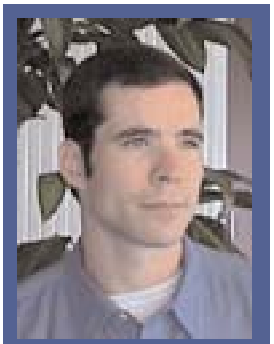
Derrick: "The money to do anything materially different than we have done up to this point is going to have to come from the federal government. Or, in our industry, the governors are going to have to tell the state regulators to allow these rates to go up considerably and I think there will be an awful lot of pushback to that."

Hutchinson: "With regard to the energy sector that you described, it's a layer protection. No one entity, private sector, state, local, or federal government can handle it all. And when I say 'layer protection', the first protection against that type of incident on a pipeline, would be knowing who comes in and out of our country, and having good intelligence as to who's trying to come in to do us harm. And if we have a good layered protection on our borders and our transportation industry, that's going to help us to protect our pipelines. The second thing is to limit vulnerability. As John pointed out, there's not one segment that's responsible for the whole thing. We do not want to have one area that destroys an entire system. So you limit the vulnerability as well. It cannot be a perfect system because we are a free society. But with that layered protection and division of responsibilities, we come up with a pretty good mosaic of protection."

Allen: "I can give an example of at least where two infrastructures working with the federal government are trying to address those interdependencies... We have been working with the telecommunications industry, the financial sector, and CEO's, to identify some of the vulnerabilities and to identify ways to recover. It's an unparalleled event where we're bringing the players together to share data. And this goes back to the information sharing, in a secure environment and an environment that allows us to share very sensitive data, and to actually look at where the vulnerabilities might be and what we need to recover together as two industries. In the end, however, it's going to take more than us. It's going to take the government and incentives to help make the changes in the telecommunications infrastructure that are needed. But there are ways that two industries can work together in very specific areas."

(Continued on Page 12)

George Mason University at Forefront of Homeland Security Efforts and Developing Models of Public and Private Cooperation



Sean Gorman

George Mason University (GMU) is actively engaged in developing strong relationships and methods of practice for coordination among government, private sector, and academia to strengthen homeland security. A clear example of the efforts underway is provided by the recent attention GMU has received concerning a research project focused on the nation's Internet infrastructure. This project, the Internet Infrastructure Study, sponsored by the Critical Infrastructure Protection (CIP) Project extends work that was begun by a doctoral student, Sean Gorman, at GMU's School of Public Policy.

Gorman began his research into the physical connections of the Internet as a master's student in October 1997. His original goal was to determine how the business and industrial sectors were connected and measure their economic impact. Gorman and GMU Public Policy Professor Laurie Schintler, Gorman's academic advisor, wanted to help create policy recommendations for mitigating the effects of an attack on infrastructure and facilities. The focus of their research was theoretical models and Gorman just happened to choose telecommunications.

Gorman and Schintler used a combination of information publicly available on the Internet and data purchased from firms to locate the infrastructure and identify the most vulnerable areas. Using raw data and mathematical calculations, they created a detailed map of the nation's telecommunications infrastructure.

"The mapping was a way to test mathematical models," Schintler said. "Our primary interest wasn't in the data, but in the modeling - how networks would behave under a set of circumstances, including reliability and resiliency. We could have chosen the interstate system or the air traffic control network."

Gorman said they initially looked at the data from an economic development perspective but after Sept. 11, began to look at it from a security perspective. He says he and Schintler had initial concerns over the significant interest by industry and government the research received, and how that interest might limit his ability to use the research in his dissertation, but those concerns were "rapidly resolved" through a series of meetings. As noted, the extension of Gorman's research was the development of the Internet Infrastructure Project, sponsored by the GMU's School of Law's Critical Infrastructure Protection (CIP) Project. The CIP Project staff coordinated opportunities for Gorman and Schintler to present the research beginning in May 2002 to government and industry officials and to address their concerns about disclosing specific, vulnerable information.

"Those early meetings allowed the research project to set up some guidelines of what would be a good idea to publish and what wouldn't, and to set up a structure of what was sensitive and what wasn't," Schintler said. "We had no problem with showing the information to government officials. We wanted to work with others to make sure that any sensitive information contained in the dissertation would not be released."

Gordon Johndroe, spokesman for the Department of Homeland Security, said in a written statement: "We're pleased that both he [Gorman] and the school have chosen not to publish the entire report because it could be used to cause us harm. But certainly it is research that should be done and it is the type of work that our own infrastructure protection unit is currently

(Continued on Page 8)

Gorman Research *(Cont. from Page 7)* involved in."

As for Gorman, he is confident he'll be able to use enough of the non-sensitive research to complete his dissertation and graduate. "This has given me quite a bit of insight into a side of policy that a graduate student doesn't often see," Gorman said. "Being involved as the process goes forward was a unique experience."

The initial media reports focused on concerns over the sensitivity of the information and how to handle this type of information. CIP Project Director John McCarthy says that ultimately the media attention helped bring groups together to address the security concerns and further a GMU mission to bring together academia, industry, and government in solving real-world problems. In addition, McCarthy says that he has received numerous inquiries from other Universities into how best to manage these types of research activities.

"The CIP project has brought together highly qualified and knowledgeable experts with significant experience in cyber security and critical infrastructure protection from the public and private sectors," McCarthy said, "along with renowned academic scholars from interdisciplinary perspectives to carefully and deliberately address this area of pressing national security."

McCarthy says the CIP Project is also cooperatively involving corporations and other private sector entities, lawmakers, and other interested parties, such as the privacy community. The result, he says, is the CIP Project is now helping to provide a means for cooperation and collaboration between government, industry and academia that is addressing a void that had been growing as various initiatives were launched, often from disparate or divergent perspectives, to develop methods for cyber security and critical infrastructure protection. McCarthy says he sees an important role for academia as a neutral third party for this type of work so public and private organizations can cooperate and share information to keep making progress, while keeping the country's critical infrastructure safe.

The CIP Project is an interdisciplinary, multi-institutional solution based research initiative which actively engages stakeholders to balance public / private incentives and integrates the disciplines of law, policy, and technology for enhancing the security of cyber networks and economic processes supporting the nation's critical infrastructures.

Laurie Schintler

The CIP Project has sponsored over 50 individual research initiatives, such as the Gorman and Schintler Internet Infrastructure Study, in the areas of Law and Economics, Public Policy, and Technology.

In addition to direct research activities, the CIP Project has sponsored various outreach activities including a monthly newsletter, and several National Conferences on topics ranging from Cyber Crime, Information Sharing and Anti-Trust, Open Source Software, National Security, University Security, Government Industry Relationships, and developing the Law and Policy National Research Agenda. The CIP Project has specifically sponsored 14 external universities, 11 Academic units within GMU, 77 research professors, and some 150 research assistants and students. ❖

GMU Professors Conduct a Post-Conflict Stabilization Study of Afghanistan

In a clear demonstration of partnering between government, industry and academia, George Mason University (GMU) Critical Infrastructure Protection Project Team Member and Research Professor from the School of Public Policy (SPP) Ted Woodcock, SPP Professors David Davis and Allison Frendak-Blume, and consultant Dr. Loren Cobb organized and conducted a post-conflict stabilization study of Afghanistan at the Swedish National Defence College in Stockholm. The GMU group with the assistance of Dr. Cobb from Colorado and Professor Hitchins from the United Kingdom is building the Strategic Management System (STRATMAS) for the Swedish National Defence College and the United States Joint Staff, J8, The Pentagon.

During the post-conflict stabilization study, STRATMAS was used to generate data on future potential societal conditions in Afghanistan and to assess the impact on those conditions of notional military and civilian groups deployed according to plans developed by the study participants. The study took place in the Aquarium facility (shown below) at the Swedish National Defence College. The Aquarium is the Swedish National Command and Control and Crisis Management Test-bed. STRATMAS has been designated as the centre of gravity of the overall Aquarium software suite by senior Defence College personnel. Anders Christensson at the Defense College is the Technical Manager for the Aquarium and the Swedish-sponsored part of the STRATMAS project. STRATMAS model-generated data as displayed in the Aquarium facility were described as "seductively realistic" by a senior participant in the study. Another senior participant stated that the data and information produced by STRATMAS were perfectly adequate to support senior military planning and decision-making activities for operations.

The Aquarium facility at Swedish National Defence College (showing SPP Professors Woodcock and Frendak-Blume, Dr. Cobb, Ambassador Farrand, and other study participants).

The STRATMAS team used two consecutive notional scenarios in the study. The first scenario described the transformation from a post-conflict situation involving high to intermediate levels of violence. It involved the deployment of the notional Afghanistan Emergency Force (AFGEM) involving some 60,000 individuals under UN Security Council authority as well as civilian humanitarian entities. The second scenario considered further transformations to low violence level conditions where societal reconstruction and development become possible. In the second scenario, a year after deployment of AFGEM, the UN Security Council notionally authorized deployment of the notional Afghanistan Recovery and Stabilization Force (AFGRES) with maximum force strength of 25,000, in order to support the recovery and long-term stabilization of the country.

The senior political leadership group at the post conflict stabilization study included Bill Farrand, a retired United States ambassador and former Supervisor of Brcko in Bosnia, and Larry Sampler who was responsible for organizing the Loya Jirga in Afghanistan. The group provided strategic political guidance to the military force commander, Major General Anders Lindstrom from Swedish Defence, and other study participants. The force commander issued command intent and planning guidance statements to the planning staff. The planning staff, consisting of military and civilian personnel, prepared 90-day action plans to represent the initial response to the conditions in Afghanistan associated with both the AFGEM and AFGRES scenarios. STRATMAS was used to assess the impact of those plans. Data on key societal variables were displayed by STRATMAS in map-based and textual formats. Those data indicated

(Continued on Page 11)

LEGAL INSIGHTS

When Sean Gorman's work hit the front page of The Washington Post, it created a stir - writ large. Those of us at the CIP Project have been dealing for some time with the smaller stir that Gorman's work creates every time it's presented. Sean, and other emerging research scholars like him, represent extremely valuable national assets and future thought leaders for providing for our nation's security.

We're proud of Gorman's work: it's truly novel, and it's truly useful. We're also concerned about its implications, just as everyone should be who understands it. It serves as a prime example of the work that spurs ongoing tension between academic freedom and national security.

The tension between academic freedom and national security has existed as long as universities and governments have existed. In the United States, it had been on the back burner for several years before Gorman turned on the spotlight. During the Cold War - in other words, in the pre-Internet era - nuclear research led to a set of rules and guidelines for handling sensitive data arising in the academic arena. One of the aims of the Atomic Energy Act of 1954[1] was to allow the government to seize and classify privately generated data relating to nuclear intelligence.

The Atomic Energy Act gave rise to a legal doctrine that was informally called "Born Classified." The Born Classified doctrine asserts that nuclear research information is classified, regardless of who created or controls it - in other words, if it contains nuclear information, it is "born classified." The last high-profile case filed under the Atomic Energy Act was a 1979 case called United States v. Progressive, Inc.[2] In Progressive, the government sought to prevent publication of an article that contained three vital pieces of information about building an H-bomb. The government obtained an injunction and was set to pursue the case fully, but publication elsewhere mooted the case before it ran its course.

Although Progressive received a lot of attention, the academic-freedom/national-security debate seemed less pressing when the Cold War fizzled and the Berlin Wall fell. It persisted in principled debates over whether, for instance, Professor Daniel Bernstein at the University of California (Berkeley) could post information about his encryption software Snuffle on the Internet (Bernstein v. Justice). An important free-speech debate, certainly; an important legal issue in terms of what constitutes "export" in the Internet era. Yet, although the Department of State's opposition to Bernstein's action was premised on a national-security argument, any consequent threat from Bernstein's postings seemed hypothetical at most.

Threats - of all kinds - no longer seem hypothetical. Digital threats seem, if anything, more potent than others: they are poorly understood, insufficiently quantified, and new.
When the Post article on Gorman was published, it gave rise to a firestorm of inquiry about how this young scholar was managing the material, and whether, in fact, universities ought to hold such material at all. It sounded like the nuclear research debate, all over again.

But this isn't the nuclear-research era, where a single issue is viewed as sensitive and its researchers are tracked. This is the Internet age. Gorman used information that anybody could have accessed. While single pieces of this material would have been interesting and useful alone, their purposeful accumulation raised national security concerns. The fact that he is operating in a university environment is irrelevant to the results he has achieved. His operating center need not - indeed, should not - be made central to the discussion. He could have accomplished the same thing outside the university setting. And this, perhaps, is more disturbing: we have no idea whether, in fact, someone else has accomplished the same thing outside the university setting. As Steven Aftergood of the Federation of American Scientists has observed, a responsible scholar faces the implications of his work and behaves accordingly - as Gorman has done.[3] What about irresponsible scholars? And terrorists?

The nation's citizens are sufficiently

(Continued on Page 11)

STRATMAS *(Cont. from Page 9)* significant reductions in violence and an amelioration of overall societal conditions resulting from deployment of AFGEM and AFGRES as well as the civilian humanitarian entities.

The Aquarium has supported the training, education, and research activities of military personnel, including those of flag officer rank, and civilians, including those of cabinet secretary and chief executive officer rank, for some five years at the Swedish National Defence College. The Aquarium provides an environment for the development, implementation, and testing of advanced situation assessment, command and control, and crisis management capabilities for Swedish military and civilian organizations. Aquarium research and development has benefited from the coordinated support from government, academic, and industrial entities. New concepts for integrated policy- and decision-making are under development. Research into Visual Interactive Languages, display methodologies, and other technologies are providing firm foundations for the capabilities needed to support envisioned future systems.

The possibility exists to acquire an Aquarium to support research and development activities at George Mason University. An Aquarium at the university could provide a visualization facility that would allow United States policy- and decision-makers to more clearly see the states and conditions of critical infrastructure systems and to develop new ways of providing protection and deterring and preventing attacks on those systems. The Aquarium could also provide new research-level facilities to visualize the states and conditions of critical infrastructure protection systems as a result of policy changes and subsequent operational impacts. The Aquarium would serve as a test-bed for the development and study of advanced critical infrastructure protection capabilities and for the training and coordination of critical infrastructure protection personnel. ❖

Insights *(Cont. from Page 10)* concerned about safety that temperatures run high when it comes to securing infrastructure-related information. This can lead, however, to a reactionary clamp down. Academic journals have a long tradition of pushing the envelope on free speech. Yet in February 2003, several editors of leading scientific journals joined in signing a statement asserting their own determination to limit publication of material that could be used by terrorists.[4] As two leading academics subsequently observed, such self-limitation "pose[s] many of the same dangers of constricting beneficial scientific research and the open exchange of information necessary to produce and confirm it" that regulation poses.[5]

In the hue and cry over security, the prize of our heritage - freedom of expression, which includes freedom to publish - has a much smaller ring. Yet if we do not preserve it, we will have lost much more than the mere contents of unpublished volumes. We will have sacrificed one of the pillars upon which our nation was built.

What to do? The academic-freedom/national-security debate did not achieve a mature legal resolution in the Cold War. Since the questions have reappeared in the complex Internet context, and we have only incomplete precedent on which to draw, the CIP Project will turn its attention to this issue for the next CIP Community Conversation. Using the approach of the first CIP Critical Conversation, the thought leaders, policymakers, and affected parties will come to the National Press Club to explore options before the nation.
Most of us today are not as single-minded as Benjamin Franklin was when he said any society that would give up a little liberty to gain a little security will deserve neither and lose both. The risks are different now, and the American attitude is different too. We manage the risk and, hopefully, minimize it; we accept what's left. As a society, we are struggling now with how much risk we can accept, but let's not fool ourselves: there will always be risk, with or without academic freedom.

❖

[1] 42 U.S.C.S. § 2011 et seq.

[2] 467 F. Supp. 990 (W.D. Wis. 1979) and 610 F. 2d 819 (7th Cir. 1979).

[3] Steven Aftergood spoke about the Gorman research in On the Media, National Public Radio, July 13, 2003.

[4] See Ronald M. Atlas et al. (group editorial), Uncensored Exchange of Scientific Results, available at http://www.pnas.org /cgi/content/full/100/4/1464 (last visited July 17, 2003).

[5] Elizabeth Rindskopf Parker and Leslie Gielow Jacobs, Government Controls of Information and Scientific Inquiry. In BIOSECURITY AND BIOTERRORISM: BIODEFENSE STRATEGY, PRACTICE, AND SCIENCE, Volume 1, Number 2, 2003.

Critical Conversation *(Cont. from Page 6)*

Hager: "Let's use the example of a nuclear power plant. When they do everything they can do and they have to call on government because protection is beyond the resources that they have available, then we step in. The feds deal with the airspace issue, the Virginia Marine Resources Commission deals with the water issue, the Virginia State Police provides a greater buffer around the plant on the land side. It's a cooperative effort. And then everybody recognizes that mores needs to be done."

Progress on Security Policy Issues

Hager: "I think we're making tremendous progress. Recognize that we'll never be totally safe and secure. Everybody says that, they know that. It's a vast country. We're a free country. So you've got to keep that in mind."

Turner: "In terms of policy, we do need a comprehensive commitment and plan to win the war on terrorism. And it involves a whole lot of things. From being sure that in terms of our international policy and our relationships, that we create a safer world so that the world doesn't keep producing folks who are ready to join Al Qaeda and other terrorist organizations. Those are the kind of fundamental issues that have got to be addressed to be sure this country does ultimately get to the point where we can declare that we have won this war and we're no longer living in fear."

Hutchinson: "In reference to the comments about the slowness of policy, I would emphasize and underscore one particular point. And that is that we were given the marching orders that you're not going to be criticized for being too bold. You will be criticized for moving to slowly and not aggressively enough. The marching orders for the Department of Homeland Security were to illustrate that. We have moved very aggressively both policy-wise, organizationally-wise, and I think strategy-wise. Whenever we are in a free society, there will always be vulnerabilities that you can point to. That is the absolute rule of American freedom. But I think that we have to be realistic, fair in our analysis, and thoughtful in our comments."

Hager: "The policy will come. But to me, Homeland Security's about leadership. You know, when we define our office, we say we're a leadership office, we're a coordination office, to work with and through others. And we're a policy office. Because policy's important. So this is an evolutionary process. And policy has to catch up; that's fine. But it is about leadership."

Audience Generated Discussion

The attendees generated substantive questions for the panel members. One question in particular that generated quite a bit of discussion was posed by Todd LaPorte from George Mason University. He asked "Is the threat of terrorism substantially permanent now, compared to what it was in the past? Is the environment permanently uncertain? And, following from that, if it is, then what incentives are necessary for the infrastructures that we continue to rely on to be designed and migrated as quickly as possible toward a resilient profile rather than one that has to be protected at great cost, and potentially cost us more than we really need?"

Todd LaPorte

Derrick: "And we're talking about limited resources and how to best use those limited resources. It's a very, very important thing. And the way you've described it is the way I think you need to look at it in order to get to where we need to get."

Allen: "Our focus is on vulnerability. There are always going to be threats. And they're going to come from many different places. But we know our vulnerabilities. And those are the ones that we are working on, not only within our industry, but - as I mentioned - cross sectorally, so that we can understand the joint vulnerabilities we might have. And, resilience is a good way to put it."

Hager: "I think we must remember that we're in a free enterprise society. And, in that society, it's

(Continued on Page 13)

Critical Conversation *(Cont. from Page 12)* our function in government to build a no-fault, collaborative environment, so that we can exchange information, so that we can inspire, if you will, people to take actions on their own - because we know that we cannot lock it down - and get more flexible, just like you're talking about, and emphasize the upfront part, as opposed to the response and recovery point."

Turner: "The effort that's going on now, of having a continuous flow of ideas that - many of which cost money - maybe not all of them, but most of them that I'm seeing come across my desk have big price tags - requires you to make some more sophisticated assessment of the threat and the vulnerability. The truth of the matter is that the threats change. They will continue to change. And how we address the vulnerabilities are not very sophisticated today. Because everybody's saying, 'we've got to do it all'. And the truth is, we know we can't afford to do it all. And number two, if we did, we might actually be wasting some money. So that's why I say we're not near the level that we need to be yet in terms of analyzing the threats and comparing them to the vulnerabilities that we have."

Final Recommendations

Finally, the discussion concluded with recommendations for what the private sector, public sector, and academia should commit to doing in the near future.

Allen: "Three things - one, a robust and effective alert system with intelligent analytics around it. Secondly, to think and very carefully balance the need for safety and soundness and security against proscriptive legislation. And lastly, a command and control center. So when and if an event occurred, it's very clear who's in charge, and who will take over, and who our key contact points will be."

Derrick: "Number one would be to create in law a role for the North American Reliability Council, which is the integrating entity for all power systems in North America. It is needed in order to continue moving forward. Secondly, and as a follow on to that, is a connectivity to the Department of Homeland Security that allows us, through NERC, as an industry, to really come to practical places in terms of this difference between getting ready and responding. In addition, I feel that there should be one or more places where we could stockpile some critical equipment."

Hager: "Certainly, I think citizen awareness is high on the list. Gaining appreciation on behalf of our citizens of the threat alert system, of the danger to this country, of what prevention is all about. Secondly, role definition of the various functions of the federal, state, and local government and private sector - and, I think the GMU project is right on target, with a great opportunity to generate a real contribution in that area. And third and final, assessment-based funding - that we don't just throw dollars because it sounds like a good idea, but we do it based on thorough assessments, and that through those assessments, we define risk and need, and then begin to meet those higher priority needs."

Turner: "If I had my wish list, the top priority would be to be sure that we have a clear, articulated and publicly supported strategy for winning the war on terrorism. And it involves a whole range of issues, in terms of our foreign policy, in terms of the issue of being sure we don't produce more Mohammed Atas. And then, a second level, in the short term, we could cause this new directorate, Information Analysis and Infrastructure Protection, to function in the way that I believe the Congress envisioned it."

Cable Risdon Photography

Frank Sesno

More than 100 people attended the panel, including many key organizations from the CIPP/GMU community, Congressional legislative directors, Washington-based technology and telecommunication organizations, various interest groups, and an impressive array of national and local media outlets. ❖

Virginia Alliance for Secure Computing and Networking

Dan Galloway, James Madison University

Dan Galloway

The Virginia Alliance for Secure Computing And Networking (VA SCAN) brings together Virginia higher education security practitioners, who develop and maintain security programs for their institutions, and researchers responsible for creating cybersecurity education and research programs.

The Alliance is a partnership between four universities: George Mason University, James Madison University, the University of Virginia, and Virginia Tech. Joining security professionals from these universities are researchers and staff from the Critical Infrastructure Protection Project (CIPP), the Commonwealth Information Security Center at JMU, and the Center for Security Information Systems at George Mason.

Representatives from other Virginia institutions, including Mary Washington College, Radford University, The Virginia Institute of Marine Science, the College of William and Mary, and Virginia Commonwealth University, advise VA SCAN partners. VA SCAN's current mission is to strengthen information technology security programs within the Commonwealth of Virginia's Higher Education community. Plans to extend outreach to K-12, as well as state and local governments are currently under consideration.

Initial product and services offerings include:

- Onsite training and security instructional materials
- Onsite consulting and "ask the expert" email service
- Web-based toolkit of security tools and best practices
- Self-assessment checklist for Commonwealth of Virginia security standards
- Information resources such as:

- a moderated mail list for general security discussions
- a VA-CIRT group for tracking new threats
- periodic information sharing meetings and workshops
- links to other information sources

These offerings are based upon the principle that the most lasting improvements to security programs can be made, not by performing security functions for organizations, but rather by educating and guiding management and staff in defining and carrying out their own security strategies and ongoing security operations.

VA SCAN's guiding principles are:

- To teach and guide clients to develop and maintain strong security programs
- To base offerings on state and federal standards that will support the objectives of federal and state information sharing
- Offerings will reflect the business need to balance security risks and other organizational priorities
- Offerings will promote the notion that security is not just a technical issue; rather, it is a concern that should be transfused into everything an organization does
- Research will be used to keep offerings on the cutting edge
- Cooperation will transcend competition

VA SCAN intends to realize immediate gains by leveraging field-proven security tools and best practices and staff expertise. Future improvements will be brought about through close linkages of these existing methods and knowledgebase with cybersecurity research, instruction, and federal and state initiatives.

To learn more about VA SCAN visit its website at: http://www.vascan.org/. You can send any specific questions and/or comments you might have to: va-scan-ervices@virginia.edu. ❖

The CIP Project is part of the National Center for Technology and Law at the George Mason University School of Law. It is a joint initiative between GMU and JMU that examines law, technology, and policy to find comprehensive solutions to the most pressing CIP issues for policy makers and critical infrastructure owners and operators. The CIP Project was launched in May 2002. The CIP Project encourages participation by representatives from all levels of government, academia, and private industry.

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 click on this link: http://listserv.gmu.edu/archives/cipp-report-l.html.