DECEMBER 2003 / VOLUME 2, NUMBER 6

THE CIP REPORT

Reflections on CIP in 2003

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*

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

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

Contact: cipp01@gmu.edu
703.993.4840

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

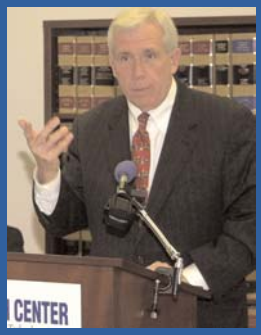
It has been seven years since critical infrastructure protection became a national priority. Over the course of that time, government, industry, and academia, both here and abroad, have engaged in new research, built partnerships, developed processes, and established new functions and organizations to perform those functions-all toward the end of protecting the critical systems upon which modern society is built. The year 2003 was no exception to the ongoing activities in governance, vulnerability and risk analysis, standards and best practices, crisis communications, R&D, outreach, and training. Not only have there been significant developments on the national level, the CIP Project too has made great strides. Just this month alone, there have been three key developments with respect to critical infrastructure protection.

Homeland Security Presidential Directive (HSPD) 7 on Critical Infrastructure Identification, Prioritization, and Protection and HSPD 8 on National Preparedness were recently promulgated by President Bush. HSPD 7 establishes a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks, superseding previous policies, including PDD 63, a seminal CIP policy document issued in 1998. HSPD 8 establishes policies to strengthen the preparedness of the United States to prevent and respond to threatened or actual domestic terrorist attacks, major disasters, and other emergencies by requiring a national domestic all-hazards preparedness goal, establishing mechanisms for improved delivery of federal preparedness assistance to state and local governments, and outlining actions to strengthen preparedness capabilities. Another important development in December was the release of the fifth and final report of the Gilmore Commission, commenting on the state of homeland security preparedness and calling for improved homeland security strategy.

This activity follows a landmark year, which marked the creation of the Department of Homeland Security and kept critical infrastructure protection in the national focus. How the developments of the past year have changed the course for critical infrastructure protection and what the future may hold are natural considerations.

We felt that it would be appropriate to close out this calendar year with the reflections of several leaders in the critical infrastructure protection community. On behalf of George Mason University, the Critical Infrastructure Protection Project, the Security Research Collaborative, and our partners at James Madison University, we wish you the happiest and safest of holidays.

Message from Congressman Frank Wolf



I am pleased to have been a part of helping to establish the Critical Infrastructure Protection Project (CIP Project) with George Mason University and James Madison University. This Project's unique integration of the disciplines of law, policy, and technology provides a necessary step to enhance the security of the nation's critical infrastructures.

The Project has hit the ground running and provided practical research and support to numerous government agencies including the White House and Departments of Homeland Security, Defense, Energy, Justice, and State. I also believe that the CIP Project's work with industry leaders from each of the critical infrastructures has provided a crucial bridge between the public and private sectors. The CIP Project has extended its reach and collaborates with a number of scholars around the nation. This effort represents the model for interdisciplinary and multi-institutional collaboration.

CIP Project sponsored research has garnered national acclaim on topics ranging from identifying Internet vulnerabilities; protecting energy infrastructure; assessing the effects of Hurricane Isabel in the Nation's Capital; and developing wargames for student cyber security curricula. It has also held two high-level, national debates, raising awareness on protecting the nation's infrastructure. The first focused on integrating public and private efforts to protect the U.S. critical infrastructures. The second debate examined the nation's electric grid in light of the blackouts in the Northeast. Key House members, industry leaders, and other national policy makers took part in these National Press Club debates.

With this track record, and unparalled level of collaboration, I expect only continued success in the year ahead.

CIPP Reflections

Dr. Linwood Rose, President
James Madison University

As a member of the National Infrastructure Advisory Commission and the president of a principle partner in the CIP Project and NSA Center of Academic Excellence, I have found the last twelve months to be a true learning and discovery period. Over the course of the past year, issues within critical infrastructure protection have increasingly been brought to the forefront of the nation's attention. A rolling blackout affected residents across the Northeast and Midwest; Hurricane Isabel brought power outages and wide swept damage to the Mid-Atlantic; and the Slammer and Sobig computer viruses attacked the country's IT infrastructure. These events and others highlight the integral role of the complex systems which provide and support the critical functions of our infrastructures. Media outlets have provided increased coverage of infrastructure failures and federal government agencies have become more active in their oversight capacity following these recent events.

As the critical infrastructure protection movement in America continues to evolve, we must come to a better understanding of the complex interdependencies of our critical systems. Research efforts which focus on multiple infrastructure sectors and the interrelated nature of these systems will help to provide more complete solutions to the problems we face in assuring the robustness of our infrastructures. Along with detailing infrastructure interdependencies, finding a balance between securing physical and cyber components of critical systems must also be achieved. Reliance on computers and other information technologies has grown at an enormous rate, often without examining the impact these advances in technology has on the physical pieces of the infrastructure. Not only must we study technological innovation, but we must find sound policy-based solutions to include the human component in assuring our critical infrastructures.

Building upon the need for a strong understanding of infrastructure interdependencies, developing new risk assessment methodologies for identifying threats and vulnerabilities to our critical systems should be brought to the forefront of future CIP efforts. The president's National Infrastructure Advisory Commission, of which I have

(Continued, Page 14)

Reflections on the State of Infrastructure Security

Paula Scalingi
President, The Scalingi Group and
Co-Director, Stony Brook University Forum on Global Security

As one of the few individuals focusing on critical infrastructure protection for the past decade, I am often asked if America is more secure today than before September 11. I always try to sound positive, but in truth the answer is "no."

Certainly, in the last year, there has been a tremendous amount of activity associated with infrastructure security. Substantial money has been spent by states, localities and industry on physical security, vulnerability assessments and identifying critical assets. There has been much media coverage on cyber threats. Multitudinous conferences and workshops on CIP have competed with exercises and training courses for the available pool of attendees. Task forces across the nation have convened to discuss potential collaborative initiatives. Yet, as a senior energy industry official vocally complained at a recent meeting, there has been much talk but little action.

Why have we made such limited headway in lessening the vulnerability of our infrastructures? The problem, in a word, is "people." Government and industry leaders are laboring under several myths that distract attention from what needs to be done.

Myth 1: Stopping Terrorism at the source is the only way to protect the homeland.

Reality. Terrorism cells are scattered throughout the world and within North America. The United States, with all its military might and wealth, cannot find and eradicate them to any significant degree. In a post September 11 world, a strong offense is no substitute for a strong defense.

Myth 2: Improving intelligence-recruiting more spies and "connecting the dots" will enable us to stop terrorists before they strike.

Reality: Intelligence at best is a national security tool, not a shield. Even with improved capabilities, we will never be able to know with certainty who the terrorists are, where they are, how they may attack, with what weapons, and when.

Myth 3: We need to identify all national "key assets" and protect our most critical facilities and components.

Reality: Our interconnected infrastructures, as underscored by the August power blackout of much of the East Coast and heartland, are vulnerable to cascading disruptions. There is no way to protect the hundreds of thousands of critical components that comprise our infrastructures. Through some modeling and simulation work underway within the federal government, we only now are beginning to appreciate the complexity of the physical and cyber vulnerabilities of these components and the linkages among them. We have a long way to go before we have developed the analytic toolset necessary to better understand interdependencies.

Myth 4: The key to energy infrastructure security is to "fix the problem" so that massive power blackouts will never happen again.

Reality: The North American energy grid is aging, increasingly fragile, buffeted by deregulation and market forces, stressed by relentlessly increasing demand, operating at near capacity with decreasing staffs and reliant on electronic components. Because of its inherent nature, this remarkable network will remain subject to disruptions. This means learning to live with risk, determining what level of risk is acceptable, and how cost-

(Continued, Page 15)

CIP Reflections: Three Issues for Academic Consideration

Sean Gorman
George Mason University School of Public Policy

Critical infrastructure protection as a US policy area had a roller coaster year in 2003. Breaking news stories like the August 2003 blackout and the computer quagmires created by a series of Internet worms kept critical infrastructure prominently in the public eye. At the same time there has been mounting concern over attention being paid by the government to the protection of critical infrastructure, especially cybersecurity. The Washington Post recently lead with the title "Cybersecurity Talk is Cheap"[1] , technology CEO's stating that, "Silicon Valley leaders worry cybersecurity seems to have slipped off the administration's radar screen." Many questions concerning critical infrastructure protection have been raised, but few answers have been delivered or endeavored. There is concern if we are even asking the right questions. Reflecting on the past year I see three questions looming over critical infrastructure protection policy that the research community could help inform: 1) Markets or regulation, and is there a middle ground?; 2) Are technology monopolies creating national security vulnerabilities?; 3) What are the pitfalls of information sharing?

The Administration's National Strategy to Secure Cyberspace largely relies on self-regulation by industry to make the necessary improvements to the nation's cyber infrastructure. The document has drawn increasing criticism by many parties, that it has not accomplished its mission. Industry believes that Washington has not done enough to back up the plan with action or funding. Meanwhile there has been strong industry resistance to any government intervention in the area. Both sides are looking for benefits without paying a cost, and that seems to be the crux of the issue - there is no cost benefit analysis or structure to cybersecurity policy making. What are the objectives of national cybersecurity and what are the incentives that will move the appropriate actors towards those objectives? What policies are the best vehicles to create effective incentives? We have a laundry list of vehicles - market forces, regulation, tort liability and contracts, voluntary standards and best practices, insurance, public disclosure, reputation/ratings, procurement[2] - but there has been no systematic analysis of what will work for cybersecurity. In many ways it appears that the answer decided what the questions were going to be. In a recent interview a high level DHS official was pressed on failures of current policies, and stated that, "Regulation is not off the table, but at the end of the day that's not where we want to be."[3] The problem is we do not know if regulation or market forces or another approach is most appropriate because the question is not being asked but reacted to. Until issues like cost benefit, objectives, and incentives have been addressed it will not be possible to chart a clear course for both government and industry to follow. I believe establishing a framework to analyze policy solutions and how they might align the nation's objectives with appropriate incentives is an area where the research community third party objectivity can help establish the necessary groundwork.

Earlier this year a report was issued entitled "CyberInsecurity: The Cost of Monopoly"[4] making the case that the dominance of Microsoft's products pose a national security risk. The report raises a very important question, but it proceeds as if the answer is a forgone conclusion. Intuitively the report's conclusions make sense, the majority of Internet worms and viruses exploit Microsoft vulnerabilities and their dominant market position makes the collective nation susceptible to these vulnerabilities. The problem is that this is an assumption

(Continued, Page 17)

Critical Infrastructure Protection - With All Deliberate Speed

James A. Lewis
Center for Strategic and International Studies

A series of reports in the mid 1990s identified critical infrastructure protection as a new concern for American security. We are coming close to a decade of study, recommendation and work on this subject, work that was accelerated (at least judging by the number of words) after the attacks of September 11th. How much progress has the U.S. made?

Surprisingly little if you take the point of departure as the Marsh Report issued in October of 1997. This is despite much hard work at all levels of government. It reflects two fundamental problems: a failure to precisely identify what is critical and what is not and a lack of progress in developing effective forms of governance for critical infrastructure protection.

The concept of criticality involves a temporal element. If there will be immediate problems when a system goes off-line, not problems that emerge weeks or months down the road, it is critical. Problems that take longer to appear allow for organizing and the marshaling of resources to respond. In a critical situation, you must respond immediately with what is on hand, placing an emphasis on preparation and planning in advance of any crisis. There is also a geographic function to criticality that is often overlooked. National infrastructures are composed of many local pieces, not all of which are equally critical or equally vulnerable. Specific parts of the larger infrastructure, or 'nodes' provide critical support, not entire networks or industries (i.e. a specific cell tower or power plant). For a period, it appeared that industries clamored to be named a critical infrastructure. The result has been a dilution of our effort as we try to defend too much. Identifying which infrastructures and which parts of these infrastructures are critical is essential for constructing an effective defense. The U.S. needs to pare and focus its list of critical infrastructure.

The blackout of the summer of 2003 helps point out where there has been progress and where gaps remain. If we take New York City as an example, we saw an excellent response by the city administration, the police and fire departments. The police moved rapidly to secure the city. However, key infrastructure nodes had not been hardened and critical local communications and transportation infrastructures failed in ways that could have been devastating in an attack. The same was true in other major cities that were affected by the blackout.

The New York subway system stopped because there was no electricity to run the trains. The subway is crucial for evacuating the city rapidly in the event of an attack with certain kinds of weapons. Mobile phone systems failed as their back-up batteries ran out after a few hours. Yet, power plants in or near New York City remained undamaged, idle only because they were unable to connect to the commercial electric grid. If there had been alternate, minimal 'backup' connections, local plants could have continued to provide power to the subway system allowing for minimal operations and speed evacuation.

Another missing concept is the hardening of critical infrastructure nodes. The model we might want to consider is hardening and redundancy used on some military aircraft or ships. It is inefficient to protect all of the aircraft or duplicate all of its systems, but it is only sensible to have backup systems in place for critical functions. If the primary control system is damaged, a secondary system that provides lesser functionality allows continued operation. The first step in critical infrastructure protection is to identify that small set of critical functions and the nodes that support them. These might

(Continued, Page 18)

Information Security and Critical Infrastructure Protection at an Inflection Point

Harris N. Miller
Information Technology Association of America

Information security and critical infrastructure protection are at an inflection point, where the hard work we have been engaged in over the past many months and years will very soon tip the balance in our favor: toward visible, meaningful results.

As these efforts pertain to cyber security, we are engaged in an environment in which cyber attacks continue to challenge our ability to anticipate and respond to them. And a vulnerable information infrastructure means vulnerability for virtually all critical infrastructures because they are so dependent on their cybersecurity elements.

But we are not without significant positive momentum to improve the situation. Among notable initiatives moving us forward:

- The Department of Homeland Security created the National Cyber Security Division (NCSD) and appointed Amit Yoran to head the Division. This goes a long way toward regaining the traction that the Federal Government lost after the White House released in February 2003 the National Strategy to Secure Cyberspace and the Department of Homeland Security (DHS) was being organized. Yoran and the NCSD will provide the leadership crucially needed to coordinate the many moving parts in critical infrastructure protection across the Federal, state and local agencies, private industry and academia.

- Industry has, for its part, enhanced its effectiveness in information sharing and coordination through the Sector Coordinator structure (ITAA is Sector Coordinator for the IT industry) and the Information Sharing and Analysis Centers. As 85% of the nation's critical infrastructures are owned and operated by the private sector, it is our responsibility to lead the effort to: develop the systems that harden our networks; share critical information among us and with the government; and coordinate strategic and tactical preparedness and response. Many of the sectors are making notable strides in this area, despite the many daunting complexities. But much more will be accomplished over the next few months when we develop clear understandings with DHS and each other about our interdependencies and synergies.

- The task described above was formally kicked off December 3 at the National Cyber Security Summit in Santa Clara, California, where 350 experts from numerous industry sectors, Federal, state and local government, and academia convened to work in partnership toward resolving 5 of the major cyber security challenges posed in the National Strategy to Secure Cyber Space: Public Awareness; Early Warning; Corporate Governance; Technical Standards; and Secure Software. This Summit was not an end to itself but the beginning of a collaborative process in which assigned task forces will target March 2004 to recommend tangible deliverables for addressing these challenges. No one expects to see any silver bullets as early as March, but we will have compiled some heavy ammunition.

- Meanwhile, Congress as a partner in this process is eager to see results faster, and is pushing industry and the government to do more. Their interest adds urgency to this collaborative process. Ultimately, all parties recognize that this process requires a policy and market environment that encourages greater attention to cyber and critical infrastructure protection, without making counterproductive, one-size-fits-all laws or regulations. *(Continued, Page 20)*

The International CIIP Handbook 2004: Findings and Prospects

Myriam Dunn and Isabelle Wigert, CIIP Research Group
Center for Security Studies, ETH Zurich, Switzerland

Critical information infrastructure protection (CIIP) has developed into a key part of national security policy during the late 90s, when a new, delicate problem became apparent: the dependency of modern industrialized societies on a wide variety of national and international information infrastructures.


Myriam Dunn

The United States was the first nation to broadly address the perceived new vulnerabilities of vital infrastructures. Following that example, countries all over the world have since taken steps of their own to understand the vulnerabilities of and threats to their *critical information infrastructure* (CII), and have proposed measures for the protection of these assets. *The International CIIP Handbook*, first published in 2002 and substantially expanded for the 2004 edition, compiles and analyzes such *governmental efforts* to protect CII.[1]

The differences in the state and quality of the protection practices in the fourteen studied countries are substantial. Nevertheless, a number of mutual key issues and major future challenges can be identified. Next to more or less well-discussed topics such as the need for better public-private-partnerships, information sharing concepts, or improved early warning schemes, two issues have emerged that have received very little scholarly attention so far and warrant focus in the year ahead. The first is the apparent difficulty to distinguish between CIP and CIIP. The second is the implications of diverse viewpoints of what is "critical" for current and future protection practices. Due to these issues as well as a lack of understanding of complex interdependencies, there is an urgent need for interdisciplinary research as a major future challenge.

CIP and CIIP as Differing but Interrelated Concepts

A focus on CIIP creates immediate difficulties for any researcher since a clear distinction between CIP and CIIP is lacking in most countries. In official publications, both terms are used inconsistently, whereby the term CIP is frequently used even if the document is actually referring to CIIP. In protection practice, CIIP is mostly handled as a subset of CIP in the sense that CIP is more than CIIP but CIIP is an essential part of CIP. There is at least one characteristic for the distinction of the two concepts: While CIP comprises all critical sectors of a nation's infrastructure, CIIP is only a subset of a comprehensive protection effort, as it focuses on the critical *information* infrastructure. It is however important that the two should not be discussed as completely separate concepts: An exclusive focus on cyber-threats that ignores important traditional physical threats is just as dangerous as the neglect of the virtual dimension.

What exactly is to be included in the CI and what in the CII is another question of difficulty: While the CI is always defined in terms of sectors and CIP as measures to secure these critical sectors of society, CII and CIIP are hardly ever defined. One could therefore argue that the distinction between CIP/CIIP is overly artificial. However, the CIP community would highly profit from a clear conceptual distinction due to several factors. First, the protection of the CII has become especially important due to an invaluable and growing role in the economic sector, an interlinking position between various infrastructure sectors, and an essential role for the functioning of other infrastructures at all times. CIIP therefore demands special attention.


Isabelle Wigert

Secondly, the system characteristics of the emerging information

(Continued, Page 13)

A Discussion of CIP Issues with Andrew Howell, Vice President of Homeland Security U.S. Chamber of Commerce

What is your opinion on how critical infrastructure protection has proceeded over the past twelve months?

The challenges of Critical Infrastructure Protection (CIP) are great, and the need to fix them urgent. Therefore, it is easy for the public at large, non-profit leaders and private sector executives to have unrealistic expectations about what can be done and what actions should be taken in the short, medium and long terms.

Because this is such a complex issue, progress in CIP this year has been slow. Rightly, the Department of Homeland Security (DHS) leadership has been focused on departmental organization and leadership issues. Before a ship can sail, it needs a captain and crew.

However, the Information Analysis and Infrastructure Protection Directorate (IAIP) has made progress in recent months in moving beyond the organizational to the policy realm. Specifically, Assistant Secretary Robert Liscouski and his team have increased outreach efforts to industry, meeting with the Sector Coordinators and representatives of Information Sharing and Analysis Centers (ISACs) that participate on the ISAC Council on a regular basis. In December, DHS was a valuable partner along with the U.S. Chamber of Commerce, the Business Software Alliance, the Information Technology Association of America and TechNet in the National Cyber Security Summit in Santa Clara, California. These efforts, among others, demonstrate the Department's commitment to working with industry to mutual benefit.

As the field of CIP evolves, what are the central issues that have recently emerged or come to the forefront?

Information security is an issue that is clearly a priority for DHS and the private sector. The National Cyber Security Summit was well received by almost everyone who attended and is a good model for public-private collaboration moving forward. The U.S. Chamber of Commerce is proud to have sponsored the summit and looks forward to working with the Awareness Task Force on developing strategies and deliverables that educate business and home users on the importance of information security.

One area, however, where the conference fell short was is in its attempts to generate cross-sector interest in information security. Clearly, we all must work to encourage greater participation beyond the traditional IT community. For companies of all types and sizes, information security is a management and governance issue that merits high-level executive attention. Explaining this is the only way to achieve greater information security and meet the awareness objectives of the National Strategy to Secure Cyberspace.

The issue of collaboration and coordination between all levels of government and the private sector takes on new importance as states identify critical infrastructure and conduct vulnerability assessments. To avoid duplication, a process is needed to coordinate these efforts with the federal effort. Additionally, some states are encouraging private sector information sharing by giving limited state FOIA exemptions. Similar legislation was passed at the federal level as part of the Homeland Security Act of 2002. However, FOIA questions still linger in the minds of many in the private sector. DHS has the opportunity to address these questions by issuing clear rules and processes concerning how it will handle FOIA protected information.

The Department of Defense (DoD) has a strong interest in and desire to secure the defense industrial base to ensure mission assurance. Therefore, it will be critical that DoD work collaboratively with DHS in areas where there is overlap.
(Continued, Page 23)

Cyber Insurance Update

By Harrison D. Oellrich, Managing Director
Guy Carpenter & Co., Inc.

In recent years, as the exposures associated with doing business in cyberspace have quickly emerged, insurers have become increasingly concerned that as these very sophisticated exposures were never contemplated, they cannot be successfully underwritten, especially within the context of traditional "bricks and mortar" property and casualty policy forms.

The recognition that these exposures are very different fuels concerns that underwriters cannot quantify, underwrite, or price for them properly. Consequently, insurers are mandating that loss from these new exposures will be tightly controlled if not entirely excluded within the traditional portfolios they reinsure. This process was well underway even prior to the attacks of 9/11, and will be reinforced as insurers and their reinsurers negotiate to renew future agreements. The knock-on impact of this to businesses is that coverage for these exposures is being dramatically curtailed if not totally eliminated from existing traditional property and casualty policies as we speak.

As insured companies grapple with the severely limited coverages likely to be available through their traditional insurance products, a new generation of insurance products focussing solely and specifically on these exposures has been developed and is already undergoing refinement. Since they are stand alone products, they allow underwriters to have the opportunity to individually assess, underwrite, and price each insureds unique internet exposures.

Present total maximum insurance marketplace limits for these products on a stand alone basis are close to $250m. However, it is extremely unlikely that more that $100m maximum can be deployed for any one insured at the present time. This is the result of insurers and their reinsurers looking to manage their limits very carefully given the present concern regarding the potential for accumulation, which we have dubbed "cyber hurricane".

For this marketplace to ever have the opportunity to reach its incredible potential, data and a methodology to model such available data will have to be developed to allow both insurers and reinsurers to have the confidence necessary to build portfolios of these new cyber exposures.

Insurers and reinsurers have spent a tremendous amount of time and resources over the last decade in an effort to quantify, through the use of sophisticated probabilistic and deterministic modeling, the actual expected losses to any existing or theoretical portfolio of risks and in just about any real or hypothetical loss scenario, be it an earthquake, windstorm, or other physical peril. Having convinced themselves that they can thus construct a portfolio of business from which they can expect an acceptable exposure to catastrophic loss from any one of these natural perils, along come these new internet exposures.

The Internet is very unique in that on the surface at least, it does not look to be able to be modeled in this way. Whereas natural perils losses occur in a specific geographical location, the Internet is both everywhere and nowhere at the same time, while the perils to be protected are still being fully identified and defined.

Consequently, in order to address the aggregation issue, a way to slice and dice the net in a similar fashion to the way traditional property cat exposures are done, i.e. by peril and geographic territory, needs to be developed. In so doing we hope to provide a framework for a future ability to model these emerging exposures so that insurers and their reinsurers will not need to aggregate every dollar of exposure from this class with every other future

(Continued, Page 21)

Reflections on Cybersecurity

Bill Guidera
Microsoft Government Affairs

The past year showed the increasing functionality and growing security challenges of the Internet. While many more people connected to the Internet through broad and narrow-band connections, we also saw another increase in the severity of malicious criminal attacks upon every major operating system. This highlights the endless pursuit of cybersecurity, which involves a daily and never-ending contest between industry, governments and computer users on the one hand, and cyber criminals, on the other. Unfortunately the global hacker community remains elusive, aggressive and innovative.

After several decades of computer security work, we know that there are no silver bullet fixes and that there will always be vulnerabilities in complex software and systems. Cybersecurity involves many layers and many collaborative partnerships, including software design, software configuration, software patching, the sharing of threat and vulnerability information, user education, user practices, and the investigation and prosecution of cybercrime both within the United States and internationally. In other words, cybersecurity involves management of technology as much as it involves the technology itself.

In recent years, consumer dependence on the Internet has grown, and consumers are more frequently sharing their personal information, including their identities, contact information, financial data and health information, over the Internet. Moreover, as the personal computer becomes more central to the lives of many citizens and to the daily functions of the public and private sectors, the government, consumers and business enterprises are storing more personal information on their Internet-connected computers and networks, thus potentially exposing their data to hackers even if that personal information is never transmitted over the Internet. As of March 2003, 30 million homes in America had a broadband connection to the Internet, double the number who had a high-speed connection at home at the end of 2001 and a 50% increase from March 2002. Broadband consumers, unlike those with dial-up connections, connect to the Internet with unvarying IP addresses and at high connection speeds, and therefore place data at greater risk if protection practices are not properly followed.

Another key change in recent years is that the time between the issuance of a patch and the time when we see a concrete exploit taking advantage of the underlying vulnerability has shortened dramatically. This time period is crucial because we have had very few attacks that precede delivery of a patch. Instead, once a patch is released, a race ensues between those installing the patch to eliminate the vulnerability and those developing code that exploits the vulnerability. When an exploit is developed faster, enterprises and individuals have that much less time to learn of, test and install the patch before a hacker uses the exploit to inflict damage. The window for the NIMDA virus was 331 days between patch release and exploit; for Blaster, it was only 26 days.

The sophistication and severity of cyberattacks are also increasing. The Slammer worm in January 2003 did not attack the data of infected systems, but resulted in a dramatic increase in network traffic worldwide and in temporary loss of Internet access for some users. When criminal hackers released the Blaster worm, it spread by exploiting a vulnerability for which we had released a patch. Infected machines then used the network connection to locate new, vulnerable machines, whereupon the worm would copy itself, infect the new machine, and continue the process. Blaster affected Windows NT4, Windows XP, Windows 2000 and Windows Server 2003 systems, but could not reach those machines that were patched and defended by a properly configured firewall. Yet with great malice, the worm writer also designed Blaster to

(Continued, Page 19)

Towards a New Appreciation of Surge Capacity: Surge Protection and Critical Infrastructure

Gregory B. Saathoff M.D.
Associate Professor of Research, University of Virginia School of Medicine
Executive Director, Critical Incident Analysis Group

Disasters are sometimes defined by their tragic irony. The following scenario is one representation of social and psychological tragedy, and illustrates the need for both surge capacity and surge protection.

During the sinking of a ship, passengers and crew safely deploy sufficient lifeboats during the night. A few of the lifeboats are equipped with specialized medical equipment and supplies in order to stabilize injured passengers. In the confusion of disembarkation, people who have minor medical problems crowd into the medically equipped lifeboats. Friends are separated. Once afloat in separate boats, however, passengers call out to each other across the choppy waves. Regrettably, some leave the security of their own boats in order to join their friends in other boats. The icy waters prove too much for some, who succumb to exhaustion after losing their bearings in the confusion. Even more catastrophic, others actually are able to swim successfully, and in the process of climbing on board, capsize the already overloaded medically equipped vessels. Rescue ships ultimately retrieve half-empty lifeboats, a stark testament to a critical failure of psychological and social response, despite adequate physical resources. The failure to suppress the surge of 'worried well' passengers to the medically equipped boats has resulted in a loss of life. How could this tragedy have been prevented? More boats? Larger boats? Availability of basic medical supplies on all lifeboats? More illumination of the scene? Enhanced communication? Greater cohesion between passengers in each lifeboat? Pre-education and planning of crew and passengers? These options represent a spectrum between actual surge capacity and the ability to engage in surge protection.

A ship of state threatened by terrorist attack can be likened to an ocean liner on the high seas. It must have the necessary physical, medical and technological critical infrastructure to deal with survival of its passengers and crew, if necessary. However, adequate resources, communications equipment and medical supplies are necessary but not sufficient for survival. The missing ingredients necessary for survival include adequate distribution of resources and the human response. How will passengers and crew utilize the components of rescue? The question is not predicated on physical resources alone. The answer entails a paradigm shift in our current understanding, and will define the success or failure of the operation.

A traditional view of surge capacity that looks only at static resources, whether medically equipped lifeboats or hospital beds, is not sufficient in planning for future terrorist events. A modern understanding of surge capacity requires us to look at resource availability in a dynamic, interdependent way. As a crisis flows, it is important to understand not only the downstream issue of surge capacity, but also the upstream issue of surge protection or mitigation. Surge occurs in crisis. While it can not be prevented, it can be proactively managed, thereby protecting the critical downstream assets that can otherwise be physically overwhelmed.

For the purpose of this article, the concept of surge suppression (a term borrowed from electronics), refers to the means to prevent damage or overload to critical infrastructure during transient spikes in usage. In our home computers, we know surge suppression by a similar name, surge protection. While we can not prevent surges, we can protect our

(Continued, Page 12)

Saathoff *(Cont. from Page 11)*
computer hardware by managing the most severe spikes that would otherwise destroy the system. Surge capacity is a more traditional medical concept, and refers to the point at which caring for patients overstresses the

health care system's ability to comfortably provide patient care. The complementary concept of 'surge protection' is therefore central to a more complete understanding of surge capacity. A thoughtful understanding of both surge capacity and protection appreciates the dynamic interplay between physical, psychological and social elements of critical infrastructure. The greater the ability for a society to be prepared to engage in surge protection, the less need is there for increased enhancement of surge capacity. It could be argued that pre-planned surge protection could have significantly reduced the more than 4,000 'worried well' healthy individuals who overwhelmed Tokyo hospitals in the hours after the 1995 release of the chemical nerve agent sarin in the Tokyo subway system.

Although the concept of surge capacity can conceivably be appreciated in the interaction of finance, communications, security, transportation, energy, and water, it is most traditionally illustrated in meeting the medical needs of a community under attack. In the medical arena, our society is faced with the real threats of domestic-based chemical, biological and radiological mass casualty situations. In the face of limited resources and constrained production capabilities, a broader understanding of the issue of surge capacity is required. Specifically, the availability and distribution of a number of resources and mechanisms is critical for a successful response to an attack. These include pharmaceuticals, medical supplies and equipment, medical personnel, hospital beds (including beds in negative pressure rooms) decontamination ability, non-medical personnel, industrial base & distribution system and manufacture-order-ship time (MOST). The successful deployment and delivery of these elements to communities in a hydraulic manner can mitigate the need for traditional inpatient bed capacity.[1]

The concept of psychological and social contagion and its impact upon critical infrastructure is important although often neglected in discussions of critical infrastructure.[2] Critical infrastructure is often geographically based, tied to existing population density and predicated upon the ability of human resources to operate, maintain and repair various aspects of that infrastructure during times of crisis. In the event of terrorist attack, our critical infrastructure will be threatened if individuals choose to flee their communities rather than to remain. If population density shifts during crisis through unplanned, spontaneous evacuation, population surges will create transient and sustained spikes in resource utilization in areas that are ill-equipped to handle the resultant stresses. Using the sarin attack as an example, the cost of building a traditional hospital system in Tokyo to absorb the surge spike of frightened citizens is clearly prohibitive. A community-based approach, built upon the model of shelter-in-place could arguably manage the surge upstream, thereby protecting essential assets for those who are most in need.

During the past two years, the Critical Incident Analysis Group (CIAG) has developed a concept called Community Shielding that has broad policy implications for public response to weapons of mass destruction. This concept entails pre-planned, community-wide shelter in place, with an emphasis on communication[3] and delivery of essential services, including medical resources, to affected populations. The National Capital Region component of the Critical Infrastructure Protection Project (CIPP), has provided the CIAG with a grant to develop metrics surrounding public attitudes toward the concept of Community Shielding. The objectives of this effort will be to survey vulnerable populations within the National Capital
(Continued, Page 22)

Dunn and Wigert *(Cont. from Page 7)* infrastructure differ radically from traditional structures in terms of scale, connectivity, and dependencies. The interlinked aspects of market forces, technological evolution, and emerging risks will likely aggravate the problem of CII in the future. This means that understanding current and future CII will require highly sophisticated analytical techniques and methodologies not yet available. This is another point that demands special attention.

What Is Considered to be "Critical"?

CIIP is an issue of high relevance in many different, very diverse, and often overlapping communities. These different groups do not necessarily agree on what constitutes the problem, on what to consider critical, and thus on what to protect. The differing positions complicate the allocation of *responsibility* when it comes to the protection of critical information infrastructures and, by implication, in defining appropriate political tools for dealing with the problem. They are reflected in the orientation of protection policies, which range from a regulatory policy focus, concerned with the smooth and routine operation of infrastructures and questions such as privacy or standards, to inclusion of CIIP into overall Counter Terrorism efforts.

Despite these differences, one striking similarity in all countries becomes apparent: static infrastructures are not the objects of protection, despite the terminology of critical *infrastructure* protection, but rather the *services*, the physical and electronic (information) *flows*, their *role and function* for society, and especially the *core values* they deliver. This is a far more abstract level of understanding essential assets which again demands new analytical tools and mindsets: While single infrastructures are relatively easily illustrated in terms of organizational and institutional hierarchies, services, flows, and values are a lot more complex, harder to capture, and far more difficult to understand.

In general, two (interlinked) types of criticality can be distinguished. The more traditional and technical view understands criticality as a structural concept. In this view, an infrastructure or an infrastructure component is critical due to its position in the whole system of infrastructures, especially so because it is an important link between other infrastructures or sectors. Lately, a more abstract view has emerged that understands criticality as a *symbolic* concept. In this view, an infrastructure or an infrastructure component is critical due to its role or function in society. This view, substantially impacted by the tragedy of 9/11, allows the integration of non-interdependent infrastructures as well as non-man-made objects into the concept of critical infrastructures.

This symbolic understanding has one major advantage over the structural one: It allows us to define existential security policy relevant assets more easily. This is of central importance since the question of criticality in the socio-political context is always inextricably linked to the question of how damage or disruption of an infrastructure would be perceived and capitalized politically. Actual loss (be it monetary or loss of lives) stands next to political damage or loss in the basic trust among the citizenry for the mechanisms that govern it. These aspects have been largely neglected in current CIIP research.

The Research Challenge

The need for assessment of CI/CII is indisputable. In order to plan adequate, cost-effective protection measures, key aspects of critical systems must be understood. But such an understanding is not at all given today: Current methods and models to analyze CI/CII exhibit significant shortcomings. The limitations of present approaches become apparent mainly in their inability to cope with the problem of complex interdependencies. They are either too sector-specific or too focused on single infrastructures. Neither do they take sufficient account of the strategic, security-related, and economic importance, nor of the potential risks affiliated with critical infrastructures, especially when they are placed within the context of the wider interdependent relationship with other critical infrastructures.

It is generally recognized that satisfactory metrics to describe the *(Continued, Page 14)*

Dunn and Wigert *(Cont. from Page 13)* danger of failures for highly interdependent infrastructures are lacking. It is also acknowledged that such a set of metrics or models would have to include economic, social, and national security considerations. This points to one fundamental issue and major challenge in terms of research: Only interdisciplinary approaches pay sufficient tribute to an issue that is *inherently* interdisciplinary.

However, the question of CIIP has received little attention from large parts of academia up to now. Research on aspects of IT-security, generally focused on the technical level and on local subsystems, is important - but it often misses crucial key features of the complex systems at hand and does not suffice to come to a problem solution. It is likely that critical vulnerabilities, and consequences of infrastructure disruptions, will not be traceable in any useful way to single technical subsystems - as a consequence of an already overwhelming system complexity. Effective protection for critical infrastructures calls for holistic and strategic threat and risk assessment at the physical, virtual and psychological levels as the basis for a comprehensive protection and survival strategy and will thus require a comprehensive and truly interdisciplinary R&D agenda encompassing fields ranging from engineering and complexity sciences to policy research, political science, and sociology. ❖

[1]Myriam Dunn and Isabelle Wigert. The International CIIP Handbook 2004: An Inventory and Analysis of Protection Policies in Fourteen Countries. (Zurich: Center for Security Studies, 2004). The book is forthcoming in February 2004 and can be order at www.isn.ethz.ch/crn. The 2002 edition is available for download at the same site. The following countries are included in the 2004 edition: Australia, Austria, Canada, Finland, France, Germany, Italy, Netherlands, New Zealand, Norway, Sweden, Switzerland, United Kingdom, and the United States.

Rose *(Cont. from Page 2)* the honor to serve, has begun to examine the issues within the risk assessment field and will produce a report detailing its findings. By conducting thorough assessments of key components within each infrastructure sector, industry and government officials will be able to determine where the greatest vulnerabilities lie and how to best correct these needs.

Lines of communication must be opened both within and across the sectors. The Information Sharing and Analysis Centers (ISACs) existing in each infrastructure sector provide an avenue for dialogue for the owners and operators of our key systems to share central issues within their industry. In order to move ahead in providing increased assuredness, it is paramount that all of the key players discuss known vulnerabilities, potential solutions, and other security related issues. Along with fostering the role of the ISACs, as a university president I am an advocate of building partnerships across the academy to study infrastructure assurance. Institutions of higher learning must be willing to collaborate to bring various areas of expertise together to build well rounded solutions.

Critical infrastructure protection has grown in importance as a national level issue. Efforts across government, industry, and academe have continued to provide solutions and advancements across the sectors. While major strides have been made in the past year, we must continue to remain focused on the goals and objectives set forth in the national strategy documents released by the Department of Homeland Security. In order to ensure a robust and resilient infrastructure cooperation is needed among all participants. At the university level, it is my goal to address the issues mentioned above and create solutions to address central issues within critical infrastructure protection. Universities can be a catalyst for positive societal change and I would like to see higher education be a driving force in the next year for expanding the knowledge and understanding of infrastructure issues as well as conducting cutting edge research within the critical infrastructure protection movement. ❖

Scalingi *(Cont. from Page 3)* effectively to limit the extent and duration of outages.

Myth 5: Adopting the "right" technologies will provide infrastructure security.

Reality: There are no silver bullets. Technologies, tools and methodologies can be useful in addressing vulnerabilities and other preparedness needs, once these needs are identified and incorporated into a risk-based security strategy.

Myth 6: The federal government should focus chiefly on the national critical infrastructure threat, while states, counties, and municipalities handle the local needs as they traditionally have done.

Reality: Securing interdependent infrastructures requires a comprehensive regional preparedness approach that includes all hazards-physical, cyber, WMD, natural disasters, accidents, systems failure, and human error. Such an approach includes protection, mitigation, response/recovery, training, exercises, and research and development. The focus must be on regions because infrastructures' services areas and their customers cross jurisdictional and national boundaries.

What needs to be done?

In the last year, there has been a growing body of data gleaned from vulnerability assessments, multidisciplinary studies, Congressionally-mandated commissions and exercises (including TOPOFF 2) on requirements necessary to better secure our infrastructures. Many of the most pressing needs are operational and focus chiefly on improving regional preparedness.

Among the most useful means to illuminate readiness shortfalls are regional public-private partnerships. A number of these collaborative initiatives have been created around the nation. Three of them have held infrastructure interdependencies exercises-the Pacific Northwest Partnership for Regional Infrastructure Security (Blue Cascades in Portland, Oregon, June 2002), the San Diego Regional Homeland Security Partnership (Golden Matrix, April 2003) and the Gulf Coast Regional Partnership for Infrastructure Security (Purple Crescent in New Orleans, October 2003). In each of these exercises, the general areas of shortfall were essentially the same:

- Limited understanding of regional interdependencies, lack of coordination among public and private sector organizations on response and recovery plans, and little, if any participation by commercial business and community organizations in preparedness planning or exercises.

- Erroneous assumptions and confusion on authorities, roles and missions; lack of a management plan for obtaining and allocating scarce personnel and equipment resources; and unrealistic procedures for evacuation or sheltering in place.

- Lack of awareness of potential impacts from attacks and disruptions, particularly from WMD on infrastructures, health and safety, and the economy; and lack of a coordinated regional public information capability to minimize panic.

Stakeholder recommended actions to address these gaps are, in many cases, low cost and achievable in the short-term. Among them are:

- Development of a regional preparedness strategy that addresses all hazards, including improvised nuclear and radiological events;

- Review and coordination of state and local response plans and mutual aid agreements with input from private sector organizations;

- Identification of federal civilian and defense resources for addressing response/recovery from WMD, as well as other attacks and hazards;

- Creation of a regional clearinghouse and database with security and access protocols for use in preparedness planning;

- Development of analytic tools for planning and damage assessment/reconstitution for stakeholder use;

- Undertaking studies of contamination of infrastructures

(Continued, Page 16)

Scalingi *(Cont. from Page 15)*
from nuclear/radiological attacks and cost-effective mitigation/reconstitution solutions;

- Creation of a secure, regional common communications and information exchange network to disseminate threat/outage-related and response information to the public;

- Incorporation of interdependencies into risk management approaches that assess the cost and benefits of mitigation options;

- Compilation of public and private sector initiatives that can be shared with regional stakeholders;

- Undertaking studies on the impact of the panic factor on response and recovery; and

- Developing a regional public information plan and establishing preparedness training courses for public and media.

Moving the Ball Down the Field

Most of the preceding needs can only be addressed with public-private sector cooperation. This means getting beyond traditional ways of doing business and determining collectively how to develop requirements, pay for and manage initiatives that require cross-sector and multiple stakeholder involvement and investment.

The lion's share of the responsibility for protecting the nation- and for the funding and technical expertise required, rests with the federal government. A greater federal leadership and facilitation role will be necessary before any measurable gains can be made in making our infrastructures more secure. To do this means jettisoning the myths that are impeding forward movement on necessary solutions and taking ownership of their implementation. It also requires speeding up the process of getting the Department of Homeland Security integrated, fully staffed, and working closely with both public and private stakeholders to develop and implement comprehensive regional preparedness plans that reflect a broader national strategy. ❖

Paula L. Scalingi is President of the Scalingi Group and Co-Director of the Stony Brook University Forum on Global Security. She previously was the founder and former director of the U.S. DOE Office of Critical Infrastructure Protection and of the Infrastructure Assurance Center at Argonne National Laboratory. Dr. Scalingi also has served as a staff member of the House Permanent Select Committee on Intelligence and as an analyst at the Central Intelligence Agency.

Gorman *(Cont. from Page 4)* and not an empirically proven fact. This might seem like academic nit picking, but the issue is very important because it is one of the few issues that government can strongly influence. Further, it strikes at the heart of the macro level forces that shape our critical infrastructures, of which 85% is privately held. Does economic efficiency result in a security negative externality, and is that security threat great enough that government needs to intervene? The answers to these questions are not always intuitive, especially when it comes to a large and complex infrastructure like the Internet. In the Microsoft case, would a less dominant market position result in a more diverse and secure Internet? The answer is a large question mark. The code red worm of 2001 specifically exploited Microsoft servers and is estimated to have caused in excess of 2.6 billion dollars in damage.[5] Yet of the 125,888,197 hosts connected to the Internet in July of 2001, code red only infected 359,000 of them, and Microsoft only accounts for about 23% of the Internet connected server market. The end result was a worm that did a large amount of damage to cyber infrastructure, but only infected a rather small part of the market. The implication being that there is not always a direct link between security vulnerabilities and market position. Does this mean the same conclusion holds true for operating systems, routers, and email applications? No. The answer is not intuitive and requires sophisticated analysis far beyond the simple example cited here, but it is an issue that looms large over critical infrastructure because it reveals the core of many infrastructure policy issues.

The last issue is not necessarily one that the research community can inform, but one they are actively participating in - the problems of information sharing. In various interactions we had through the CIP Project with government and industry stakeholders, information sharing has been a bottleneck at every juncture. The government wants an inventory of critical infrastructure and vulnerabilities, and industry operators do not want to provide the data. The reasons given for not providing information to the government typically revolve around fears of it being divulged through the Freedom of Information Act and the resulting security implications. I've always found this rationale confusing. The core of our research has been the collection and analysis of infrastructure data, where fiber optic lines, power transmission lines, switching facilities, etc. are located. The one resounding thing I've learned in the process is that there is a lot of detailed information available to the public, both for a fee and for free. At a press club event on the power grid I asked the panel, if the data is already out in the public domain then what is the reason for not sharing data with the government to reduce the existing vulnerabilities? The answer was a combination of the companies that sell the data should be outlawed and the data they have is from before September 2001 and now outdated. Unfortunately there is no way to put the genie back in the bottle, data is in circulation, and as much as we would like it to become quickly out of date, the amount of new build outs in sectors like telecommunications and electric power since 2001 have been minimal.

Why then the fierce reluctance to share information with the government on such a critical issue? In some cases I would hypothesize it is a strong fear of regulation. During some recent research I came across a court case involving a large telecommunications provider in the northeast. During the court case an expert witness from the provider stated that only 10% of the fiber rings in the state were fully redundant, and 90% are at least partially collapsed and vulnerable to single cut failures. Further, the standard operating procedure for restoring a failed line is to locate the lead engineer for the region, consult paper maps, manually identify an alternate route, and send technicians to wire jumpers around the outage.[6] I would imagine if this type of information were released in mass it would be perceived as a problem in need of a solution. Is it a problem that affects all providers across infrastructures? I hope not, but until the data is assessed in a joint environment it remains an open question. Security through obscurity is a panacea doomed to failure and *(Continued, Page 18)*

Gorman *(Cont. from Page 17)* the hope that bad actors will not be able to exploit available data if we pretend it is not available is a dangerous path. In short the FOIA and security excuses need to be removed as obstacles and the issue confronted directly. Only then can an answer to the problem be found, whether it is appropriating money to fix vulnerabilities - more fully redundant rings and automated emergency response procedures - regulation, standards, or a new policy innovation.

All three of these topics rely on close cooperation of government, industry, and academia. None of the issues have easy or intuitive solutions. I believe great progress has been made elevating the issue to one of national prominence and hope increased cooperation can begin to solve many of the problems facing the security of the nation's critical infrastructure. ❖

[1]http://www.washingtonpost.com/wp-dyn/articles/A31089-2003Dec3.html

[2]Hunker, J., 2002, Policy challenges in building dependability in global infrastructures. *Computers & Security* 21 (8): 705-711.

[3]http://www.eweek.com/print_article/0,3048,a=113862,00.asp

[4]http://www.ccianet.org/papers/cyberinsecurity.pdf

[5]http://www.caida.org/outreach/papers/2002/codered/

[6]http://www.state.me.us/mpuc/misctranscripts/2002-243%20080503.htm

---

Lewis *(Cont. from Page 5)* entail public safety, health care, electrical power generation and communications.

A serious defense would identify specific individual nodes in the infrastructure; assess their vulnerability and importance and then rank them in order of importance. Infrastructures that support large urban areas or are collocated with military facilities or important industrial plants would be more important and should receive Federal assistance. These key facilities could be 'hardened' by building redundancy, developing contingency plans, ensuring the existence of non-networked controls, and adding additional monitoring of functions. In the New York City example, key cell phone towers - such as those located near police stations or hospitals - could be hardened through additional power supplies or connection to an auxiliary power network, while other towers were left unhardened.

Mapping critical infrastructure has been a Federal objective for some time. An initial effort by the Critical Infrastructure Assurance Office was derailed by the reorganization of the Department of Homeland Security, but DHS has restarted the effort. A graduate student at GMU was able to assemble a map based on public documents; perhaps DHS could use this as a starting point. At a minimum, the Department of Homeland Security might want to recommend to local and regional governments that they undertake this assessment. DHS could then recommend that key facilities adopt appropriate hardening measures based on the vulnerabilities that were identified and discovered.

In this light, the decision by DHS to subsume and more fully integrate cyber security into the larger critical infrastructure effort, although criticized by many, was the right thing to do. Cyber security only makes sense as a part of a critical infrastructure protection strategy.

An effective national strategy would identify key infrastructure nodes to allow DHS to prioritize and better allocate resources and decide where to impose higher standards of security. This would ease any potential regulatory burden and the debate over government's role. Not all industries and infrastructures must be hardened or held to higher security standards. The mechanism for developing these standards could be left to the private sector, but enforcement and compliance would be a government function. The issue for governance is to find a new model for blending private and public sector responsibilities.

Creating a new style of governance remains a problem for critical infrastructure protection. Initial assessments that heavy Federal mandates and command and control regulation would be *(Continued, Page 19)*

Lewis *(Cont. from Page 18)* inappropriate were right. However, voluntary efforts will not work in a timely fashion and may not provide sufficient protection, even if guided by Federal exhortation and information sharing. It may not even be in the national interest to rely on voluntary efforts. We want companies to become more efficient. Eliminating redundancy and investing capital in functions that provide the best return are in the long term economic and security interests of this country. This works against critical infrastructure protection, however.

One model for improvement could be based on recent work in the electric power industry. The leading industry group, the North American Electric Reliability Council (NERC) prepared at the government's request a set of minimum requirements to ensure computer network security for grid reliability and market operations. These requirements were included in draft regulations issued by the Federal Energy Regulatory Commission (FERC) for public comment. While the final rulemaking has been delayed, NERC members are moving ahead with development and implementation. This experience suggests that industry-prepared standards for critical infrastructure protection, after public review, could be incorporated or recognized by Federal regulations. Compliance would be mandatory, through a self-certification process backed by Federal authority.

This blend of industry-developed standards, self-certification and federally backed enforcement avoids problems found with prescriptive regulations or a purely voluntary approach. Government agencies can be slow in developing technically proficient standards. Private sector groups are weak on enforcing voluntary standards. This more complex governance model moves beyond a purely voluntary approach by reinforcing private sector action security with strong compliance mechanisms for a subset of the current critical infrastructure sectors where a stronger approach is warranted.

The U.S. is engaged in a major reorientation of its security policies. This reorientation has major ramifications for domestic activities in a way that previous security policies did not, in large part because of the emphasis on critical infrastructure protection. Recognizing this, the U.S. must now move in the upcoming months by locating crucial infrastructure nodes and, in the context of a strategy that sets priorities and allocates resources, hardening them to resist attack and disruption. ❖

Guidera *(Cont. from Page 10)* deny service to those who sought to download the patch we created to protect them from the attack.

In response to these evolving threats, industry significantly increased the resources and priority it devotes to cybersecurity issues. Many of those efforts are ongoing and being conducted in partnership with government.

First and foremost, we welcome the National Cyber Security Division (NCSD) at the Department of Homeland Security. The NCSD's recent Cyber Security Summit showed their leadership and tremendous value in addressing these issues, and my colleague Scott Charney proudly accepted a co-chairmanship role in one of the Summit's key task forces. Many of us in industry are also working closely with Congress and agencies such as the Federal Trade Commission and the Department of Justice to address the broad array of issues, including raising awareness for consumers, investigating criminal attacks and developing new public policies. These actions are important steps in our shared perpetual journey toward enhanced cybersecurity.

Within Microsoft, we recognize that many of our customers have been affected by worms and viruses. As a result, security is our top priority and has been since Bill Gates launched our Trustworthy Computing initiative in January 2002.

The Trustworthy Computing goals are real and specific, and this effort is ingrained in our culture and the way we value our work. We have expanded the training of our developers to put security at the heart of software design and at the foundation of the development process. All new software releases and service
(Continued, Page 20)

Guidera *(Cont. from Page 19)*
packs are now subject to an enhanced security release process which has already resulted in a notable decline of vulnerabilities in some of our server software. For example, if you compare Windows Server 2000 and Windows Server 2003, for the last six months, Windows 2003 has required fewer patches.

Another part of Trustworthy Computing involves communicating with our customers. In the wake of Blaster, we launched the Protect Your PC campaign, urging people to take three steps to improve their security all available through www.microsoft.com/protect. I encourage you to share this site with others to ensure that they are following good computer security practices, including patching, using firewall and antivirus software, and using strong passwords.

We will continue to pursue Trustworthy Computing and to work closely with our industry, government and consumer partners to enhance cybersecurity. In the end, a shared commitment to reducing cybersecurity risks and a coordinated response to cybersecurity threats of all kinds - one that is based on dialogue and cooperation between the public and private sectors - offers the greatest hope for protecting the privacy of consumer data, enhancing the confidence of consumers in the Internet, and fostering the growth of a vibrant, trustworthy online economy. ❖

Miller *(Cont. from Page 6)*
So, at this inflection point, what will it take to tip the balance in our favor? I suggest:

- Coordinated management and implementation of information security policy - among government agencies, within the private sector, and between the two;
- CEO/CFO-level attention within the enterprise to cyber security requirements to drive security investment and management;
- More research and innovation, for simplicity and return on investment;
- A positive policy environment, meaning: no technology mandates; funding for collaboration; and investment incentives.

For our part, ITAA is stepping up with significant contributions, including:

- Creation of an Online ID Theft Coalition to stem the rising tide of identity theft online;
- Coordination of the National Cyber Security Summit in December with DHS and other industry cosponsors - the first "Big Tent" results-oriented project;
- Development of a National Cyber Security Survey to measure the "public health" of America's information security preparedness at all levels of the enterprise;
- My election as Chair of the Sector Coordinator Council as governing body of the Partnership for Critical Infrastructure Security (PCIS);
- Development of a web-based information security awareness certification test, which measures the average user's understanding of his or her cyber security responsibilities

Information security is a lynchpin of homeland and economic security. Incentives to strengthen homeland cyber defense are driving industry efforts to continue building partnerships with government organizations at all levels. At a minimum, ITAA is committed to the recognition of the following principles:

- Industry owns and operates most of this infrastructure and, therefore, is its natural steward for safety and security issues;
- Government and industry share an interest in the health and growth of the Internet and e-Commerce and must find common ground on which to coordinate on critical information infrastructure protection issues;
- Government entities at the federal, state, and local levels need to better coordinate their national security activities in order to improve coordination and cooperation with the private sector;
- "Cyber ethics" must become a regular and understandable part of the Internet lexicon. Ethical online behavior must be taught at home, in school and in the workplace; and
- Government and industry share an interest in addressing critical infrastructure assurance issues on a global basis.

Together, we are closing the gap. ❖

Oellrich *(Cont. from Page 9)* dollar of exposure they will put on the books. Our initial attempt to do so has been well received by worldwide property catastrophe reinsurers who have validated a concept we have put forward for doing so by fully subscribing the first "Cyber Hurricane" Cover put into the market.

Data needed to populate insurers and reinsurers models for bricks and mortar property catastrophe exposures is plentiful, while historical data to build and run future models for these new exposures is virtually non-existent. In fact many past attacks have probably never even been reported at all, because companies are fearful of sharing information about cyber crime and attack, since their reputation with customers can be seriously damaged if customers believe on-line transactions may not be secure.

With credible data and a way to model the exposures, there is every opportunity to build a substantive and sustainable reinsurance marketplace to support these products for insurers, reinsurers, and their respective clients. To that end, a number of stakeholders in the nascent cyber marketplace have been working closely with various agencies of the executive branch of our federal government as part of a series of joint public/private collaborative efforts designed to strengthen network security. Since the government utilizes the net in the very same way as the private sector, the Internet has been designated as one of the key components of our nation's critical infrastructure that must be protected from attack at all costs.

This said, it is clearly in the government's interest to support efforts to develop a working marketplace for these exposures. Government has recognized that the protocols and disciplines which the insurance and reinsurance marketplaces can provide are exactly the same as those government wishes to impose in order to create a more secure network environment. Consequently, we hope that we will soon be able to share data gathered by various government agencies and perhaps even to explore methodologies they use to model these unique exposures.

To close, here is "a vision for the future" shared by many in this emerging marketplace. In a very short period of time, if not already at present, every business will need to have a presence on the Internet. This will mean that each will have to manage these unique emerging exposures. An apt analogy is that networks are "the buildings of the 21st century" and that even as a modern day business would never contemplate foregoing the purchase of its traditional property and liability insurances, in the not too distant future businesses will similarly need to buy specific policies covering their activities in cyberspace.

Like everything else involving the Internet, the opportunities here will arise very quickly, and form exposures never before contemplated. Insurers and reinsurers will need to be nimble and creative to fully capitalize on these very real, and significant opportunities, and all against the backdrop of our industry being able to do our part in protecting the nation's critical infrastructure against the possibility of future attack! ❖

"In 2004, I believe one emphasis should be an expansion of the bio-terrorist focus to include bio-industry. Bio-industry represents nearly 40% of global GDP I understand and maybe even more when all of agriculture is included."

Roger Stough
GMU School of Public Policy

Saatfhoff *(Cont. from Page 12)*
Region in order to assess current understanding of individual and community needs. This will assist in the development of implementation strategies that utilize overlapping communication and social networks. In doing so, a model of surge protection will be developed in order to mitigate the need for unnecessary surge capacity.

The goals of providing effective surge capacity and surge protection must be met by utilizing both top-down and bottom up strategies. While distinct, these two approaches are also complementary. Leadership and top-down planning are essential for the development of adequate surge capacity within the critical infrastructure of the health care system. While this central aspect of federal planning is vital, the physical, psychological and social value of de-centralization must not be overlooked. "Centralization of functions and decision-making in the national government may also be poor counter-terrorism policy. Populations are better protected by redundancy than by centralization, since redundancy permits most units to continue functioning even after some are damaged or destroyed."[4]

This redundancy is perhaps best represented by individual households, neighborhoods and communities. As Barkun has described, the multiple layers of the shielding model consist of households, local communities, states and the federal government. This complementary 'bottom-up' strategy recognizes that households are the fundamental units in the event of a terrorist attack. The household's ability to manage the lives of its members is critical, and its success constitutes the 'upstream' surge protection previously described. The next higher level of government, social, medical resources should not be utilized during crisis unless absolutely necessary.[5]

What are the social networks by which our society can develop strategies, community by community? Recent discussions with federal, state and local leadership indicate the value in governmental and non-governmental networks. Examples of these trusted networks include faith-based initiatives, the American Red Cross and the Department of Veterans' Affairs.[6] Although these entities have different goals, they are effective because they each maintain strong networks of trust that have been developed organically over a period of generations. Through provision of physical, social, psychological and spiritual needs, networks like these will be critical for engaging the necessary surge protection for communities that do not require targeted evacuation. The current Critical Infrastructure Protection Project within the National Capital Region is in a position to examine the metrics of surge protection through community shielding in order to enhance the existing surge capacity of our critical infrastructure.

Our country was founded by individuals who recognized the limitations of a top-down model, and the advantages of informing and involving individuals in governmental decisions. Jefferson's admonition retains its relevance today:

"I know no safe depository of the ultimate powers of the society but the people themselves; and if we think them not enlightened enough to exercise their control with a wholesome discretion, the remedy is not to take it from them, but to inform their discretion." ❖

[1]Roswell, R, Undersecretary for Health, Department of Veterans' Affairs, personal communication.

[2]Saathoff, G. Everly,G Psychological Challenges of Bioterror: Containing Contagion, International Journal of Emergency Mental Health, volume 4, number 4, 2002, pp. 245-252.

[3]Rowan, F, Public Participation and Risk Communication, International Journal of Emergency Mental Health, volume 4, number 4, 2002, pp. 253-258.

[4]Terwilliger, G. et. al., "The War on Terrorism: Law Enforcement or National Security?" National Security White Papers, The Federalist Society, www.fed-soc.org/Publications/Terrorism/militarytribunals.htm.

[5]Barkun, M., Community Shielding and the Political System, International Journal of Emergency Mental Health, volume 4, number 4, 2002, pp. 265-270.

[6]Kicklighter, M, Assistant Secretary for Policy and Planning, Department of Veterans' Affairs, personal communication.

Howell *(Cont. from Page 8)*

Are there any particular initiatives or sectors that should be emulated?

Every critical infrastructure sector recognizes its role in helping ensure homeland security. Competitors within sectors frequently cooperate in security matters since they recognize that the health of their individual company depends on the health and security of the sector as a whole. The North American Electric Reliability Council within the electric utilities community and both the National Communications System and the National Security Telecommunications Advisory Committee, within the telecommunications industry, have long traditions of excellence.

Additionally, the work and progress of the Financial Services Sector deserves recognition. Under the leadership of Sector Coordinator Rhonda MacLean, an executive of Bank of America, the sector established the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security. By reaching out to multiple trade organizations within the sector, the Council truly is working on behalf of this large, complex and diverse sector. The underlying goal is to reach the members of these organizations, educate them as to why critical infrastructure protection is important, and gain their input on how the sector should advance its homeland security objectives.

These efforts recently bore fruit when the Financial Services Sector launched its "next generation" Information Sharing and Analysis Center (FS-ISAC). The FS-ISAC establishes tiered membership levels and enables companies to receive alert information without paying a membership fee. As a result, the sector has increased the depth of information sharing, which should lead to greater security.

What are the main challenges that should be addressed in 2004?

The biggest challenge of all is clearly balancing economic security with homeland security. Doing this requires continued close collaboration between the public and private sectors at the national level, and building these partnerships at the state and local level. To adequately manage the homeland security risks we face each and every day, we must also find ways to improve and streamline information sharing. ❖

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

If you would like to be added to the distribution list for The CIP Report, please click on this link: http://listserv.gmu.edu/archives/cipp-report-l.html.