The CIP Report

VOLUME 1, ISSUE 2 AUGUST 2002

Insurance Issue

What's Inside

CIP Project Staff

John A. McCarthy
Executive Director

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

Ken Newbold
JMU Outreach Coordinator/ JMU CIP Project Liaison

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

Rebecca Luria
Project Administrator/ Executive Assistant

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

Relevance of the Insurance Sector to National CIP

The insurance sector is an integral part of the nation's critical infrastructure and cyber-security strategy. As the Federal government develops short- and long-term strategies for enhancing the cyber-security of our critical infrastructures, it must additionally leverage market forces that generate appropriate risk management practices; in addition, the government must also promote security enhancements given limited resources and knowledge on complex technological and business-process issues.

The emerging cyber exposures now associated with the nation's critical infrastructures are forcing the insurance industry to address complex issues related to coverage. Unlike traditional "brick and mortar" property, cyber risks are often intangible. However, they can result in very tangible losses--some place losses caused by the Love Bug virus as high as $10 billion. Losses caused by cyber exposures are not often covered under traditional policies, and the insurance industry is in the

(Continued, Page 4)

THE TECH CENTER
National Center for Technology & Law

CRITICAL INFRASTRUCTURE PROTECTION PROJECT

CIP Project Insurance Working Group Overview

The Insurance Working Group, working with government and industry representatives from the insurance and financial services sectors, along with several academic institutions and academicians, has developed a number of research activities that will evaluate cyber security, insurance risk modeling, and financial transactions and the internet. A quick look at emerging research activities from this group include:

- Evaluating the market feasibility and security impact of different mixes of supply or demand side responsivity in the energy sector.
- Studying internet infrastructure capacity and its subsequent traffic effects on banking and financial transactions to

(Continued, Page 3)

Critical Infrastructure and the Rise of Complex Terrorism

by Dr. Laurie Schintler, The School of Public Policy, George Mason University

September 11 brought about a greater awareness of the susceptibility of the United States to attack from ill-intentioned forces operating around the globe. In a recent *Foreign Policy* article, entitled "The Rise of Complex Terrorism", Thomas Homer-Dixon writes about this and more generally, the growing vulnerability of wealthy, developed nations like the United States to terrorism and to the psychological and financial repercussions of these acts. The author portrays a new image of terrorism, one in which the perpetrators are "techies" utilizing advanced technologies to facilitate their misdeeds and the targets, those nations that have contributed to the development and rapid diffusion of these technologies. He puts forth a compelling thesis: the vulnerabilities and risks faced by the developed world today are largely the product of the technological and economic innovations that they themselves have advanced.

First, advancements in technology have given terrorists a wider and potentially more dangerous arsenal of weapons to work with, according to Homer-Dixon. Terrorists today have at their hands what Homer-Dixon terms "weapons of mass disruption." One of these tools is the virtually ubiquitous Internet, which has become a fantastic mechanism for communicating and gathering intelligence. The web offers a plethora of information that could be used by terrorists to help plan and execute an attack – e.g., satellite imagery of major metropolitan areas, detailed descriptions on how to assemble various types of explosive devices, passenger rail schedules and routes, the structural design properties and layouts of major buildings and facilities and until recently, the location of every pipeline in the United States. Although not discussed in the article, this reality clearly brings into question whether or not for the purpose of national security the government should regulate content on the web, or impose limitations on who can access certain information. Of course, there is also the issue of who should have access to critical data.

Homer-Dixon also argues that the Internet has facilitated terrorist operations by enabling real-time communication across geographical boundaries -- i.e., groups and individuals can send and receive messages instantaneously regardless of where they are physically located in the world. There is a lot of evidence to suggest that terrorists relied heavily on e-mail correspondence in the days and weeks prior to the September 11 attack and that they are becoming more sophisticated in their use of the Internet as a means for exchanging information. The terrorists recently arrested for planning to blow up the U.S. Embassy in Paris had communicated with one another utilizing photos and video with embedded messages decoded with encryption software.

Advancements in technology are enhancing the destructive power of terrorists in other ways as well, according to Homer-Dixon. Traditional devices, such as land mines, assault rifles, light mortars and grenade launchers have become more accurate and deadly and high-tech objects that were once not perceived as weapons are now seen as "weapons of mass disruption." The clever use of jets on September 11 is offered as an excellent case in point. Rail cars or semi-trucks carrying toxic or explosive materials are also targets of attack. Vehicles that utilize containers, a fairly recent technological innovation, are especially at risk as they can be tracked and subsequently hijacked for criminal purposes.

Second, Homer-Dixon argues that the vulnerabilities and risks faced by modern society also lie in the economic and social systems that have evolved in this part of the world as a result of technological innovation. In particular, economic progress has contributed to a high degree of societal interconnectedness, spatial clustering of critical infrastructure and the emergence of sophisticated networks. Backbone networks, and the infrastructure necessary for their operation, tend to agglomerate in metropolitan areas where high technology firms, producer services, and affluent individuals are concentrated. These cities serve as gateways to the global economy. Within cities, there is a similar clustering of information technologies and networks. In New York City, for example, financial and banking services tend to be located in fiber lit buildings, or in and around "telecommunications hotels" that house network access points, Internet exchanges and collocation facilities. Networks are interconnected and spatially concentrated in other ways as well.

(Continued, Page 6)

Insurance Working Group *(continued from Page 1)* derive a set of policy and planning recommendations on how best to mitigate catastrophic and cascading effects that could occur as the result of a targeted physical and/or cyber attack on the nation's telecommunications infrastructure.

- Designing a proof-of-concept prototype to identify cyber attackers based on their "digital attack fingerprints."
- Developing an integrated operational risk management process for insurance risk modeling and actuarial data gathering activities. This focuses on identifying, measuring and correlating computer security risks. The project aims to quantify cyber-risks from the perspectives of operator error, security software efficacy, and system architecture.

As can be seen from this list of activities, the insurance working group is working in an interdisciplinary fashion in attempting to address cyber security and critical infrastructure protection issues. As these activities begin to produce information and results, this working group will further develop and refine future research activities.

GOVERNMENT LEADERSHIP HIGHLIGHT

Kenneth I. Juster &
John S. Tritak

Co-Chairs of the Insurance and Reinsurance Working Group
President's Critical Infrastructure Protection Board

Ken Juster, Under Secretary of Commerce for Industry and Security, and John Tritak, Director of the Critical Infrastructure Assurance Office, are co-chairs of the President's Critical Infrastructure Protection Board's Insurance and Reinsurance Working Group, which includes representatives from government, private industry, and academia. The group is part of the Standing Committee on Private Sector and State/Local Government Outreach. There are currently five items on the Insurance and Reinsurance Working Group's agenda.

- Sector Input to the *National Strategy for Cyberspace Security*: In cooperation with industry, the group is working on a section outlining the plan for addressing cyber risks and vulnerabilities in the insurance sector.
- Cyber Security Awareness Brochure: The group is considering creating a cyber security awareness brochure for senior management and boards of directors in the insurance industry.
- Pending Cyber Security Legislation: The group is examining pending legislation on insurance coverage (S. 2600) and the question of whether the legislation extends to cyber risks.
- Cyber Risk Modeling: The group is discussing the development of methods for accurately estimating cyber risks and the type of information that would be required to perform such risk modeling.
- Outreach to Home Users: The group is considering outreach to individual users to warn of the dangers of identity theft.

Terrorism Insurance Goes to Conference on the Hill

The terrorist attacks of 9/11 had an unintended consequence on the U.S. insurance sector leaving multiple businesses, including construction projects, small businesses, and large commercial concerns without insurance protection against another attack. With the industry reeling under $50 billion in payments for the 9/11 attacks, many reinsurers discontinued covering acts of terrorism, which has had rippling effects throughout the insurance sector and the broader economy.

For months now, Congress has been debating legislation that establishes the government as an "insurer of last resort," providing insurance companies with billions of dollars in government funds to help pay for claims from future terrorist attacks. Business leaders back the legislation and suggest that absent this federal backstop, it will be impossible to put a cap on the maximum loss the industry will have to pay out in future attacks.

Under the Senate bill (S. 2600), which was passed in June 2002, insurance companies would have to pay a portion of the claims depending on the size of the insurer's market share. The government would then pay 80% of the remaining claims for an attack causing less than $10 billion in claims, and 90% if claims surpass $10 billion. The House bill (H.R. 3210), which passed in December 2001, would require insurers to cover the first $1 billion in claims, with the government covering 90% of the additional claims. Under the House bill, insurers and policyholders would eventually have to repay the government.

Some of the most contentious issues include tort reform, limits on punitive damages, and the question of "payback." Conferees have been named from both the House and the Senate to address these differences when Congress reconvenes for its autumn legislative session.

Insurance Sector and CIP *(continued from Page 1)*
process of developing and refining insurance products specifically covering cyber exposures.

Attacks against various components of our critical infrastructure can be of either a physical or digital nature. If we are not protected against such attacks, the potential for devastation increases exponentially.

Harrison D. Oellrich, Managing Director Guy Carpenter & Company, Inc.

There are at least three key benefits for the government to work with representatives from the reinsurance, insurance, brokerage and related communities (e.g., actuarial, risk managers). First, reinsurance and insurance objectivities will foster and enhance cyber-security across the nation's critical business communities. Since 1998, the Federal government has consistently argued for enhancing cyber-security through market-based solutions. Sector constituents include representative companies across multiple insurance communities, including property, catastrophe, Directors and Officers, Errors and Omissions (fiduciary), and surety (crime). Each plays a leadership role and

The risk of cyber attack is as bad as you think it is, and possibly a lot worse.

Ty R. Sagalow, Executive Vice President and Chief Underwriting Officer, AIG e - Business Risk Solutions

offers non-regulatory options for identifying, quantifying, and managing evolving threats and vulnerabilities – with market-based penalties for
(Continued, Page 5)

Insurance Sector and CIP *(continued from Page 4)* failure to secure vital infrastructure systems and networks.

Second, these communities contribute knowledge for safeguarding critical infrastructure systems. Business owners must manage risk with limited resources. How we choose to leverage these resources, both as a business community and as a nation, is a significant national challenge. In partnering with the sector, both government and industry will benefit from a sophisticated dialogue – especially with actuarial and modeling components of the sector.

Since our physical and cyber infrastructures are only as strong as the weakest link in this highly interdependent network chain, it is important that companies forge partnerships with one another, as well as with federal, state, and local governments and law enforcement. Working together, we will be more successful in understanding and identifying known vulnerabilities and managing the ever-expanding universe of cyber threats, including cyber terrorism.

Jeffrey Grange, Vice President, Chubb Department of Financial Institutions

Third, the insurance sector contributes to national economic security in developing risk transfer options and capabilities. National economic security requires mechanisms to transfer risk. Critical infrastructure owners and operators, which include State & local governments, each require the ability to purchase risk transfer instruments in order to engage in business transactions. The President's Critical Infrastructure Protection Board (The Board) is required to develop a long-term strategy for national economic security and can leverage major sector companies to discuss the importance of developing risk capacity for furthering national economic goals and policies. *--Lee M. Zeichner, President, LegalNet Works, Inc.*

Because the Internet is so interconnected, there is the perception that a single attack could potentially affect many thousands of businesses across many different networks. Such a massive loss would affect the economy much as a catastrophic hurricane or earthquake would.

Sandy G. Hauserman
Senior Vice President
Guy Carpenter & Company, Inc.

Links to Organizations Active in the CIP Arena

AIG eBusiness Risk Solutions
http://www.aignetadvantage.com
American Insurance Association
http://www.aiadc.org
American Re Broker Market
http://amre.com
AON Financial Services Group
http://www.aon.com
Chubb Group of Insurance Companies
http://www.chubb.com/businesses/dfi/cyber/index.html
Converium
http://www.converium.com
General Cologne Re
http://www.gcr.com
Guy Carpenter
http://www.guycarp.com
National Assoc of Corporate Directors
http://www.nacdonline.org
Swiss Re
http://www.swissre.com
Marsh FINPRO
http://mmc.com/index3.html
Odyssey Re
http://www.odysseyre.com
Reinsurance Association of America
http://www.raanet.org
Risk and Insurance Management Society
http://www.rims.org
Zurich North America Financial Services
http://www.zurich.com

The CIP Project Working Groups

Based on a concept paper by Dean Mark Grady (GMU School of Law) endorsed by CIP Project representatives throughout GMU and JMU, the working groups will adopt a solutions-based approach for research identification and proposal development. The working groups will define the research agenda, activities, and deliverables, and will conduct basic research to solve the problems of how to reduce or eliminate the legal and policy barriers to implementing robust security measures against cyber-threats to the nations critical infrastructures.

The initial working groups have formed under the solutions-based headings of: Insurance, Public-Private Regulation, Civil Liability, Law Enforcement and Cyber crime, and Risk Analysis. Each of these working groups has begun work and made significant progress in developing research proposals. As an example of the working group efforts the following research proposals, which have received significant endorsement from government and industry, are highlighted.

- The Public Private Regulation Working Group has responded to a call from the White House to analyze the Defense Information Services Agency's network reconstitution efforts of the Stock Exchange in the wake of the 9/11 attack on the World Trade Center.
- The Civil Liability Working Group is involved in developing research focused on the security needs and risk mitigation strategies for network operating centers. This effort will be focused on developing a security program and process for the universities, a "Secure U." This research activity will focus on cyber security policies, practices, and cyber system technologies that are appropriate for research universities in preventing cyber attacks and cyber terrorist activity.
- The Cyber Crime Working Group is considering a proposal from the State Department to study the implications of international IT treaties.

These working groups will work closely together to ensure that the CIP Project's legal, technological, and policy research activities and deliverables are integrated into a comprehensive system for reducing cyber-threats to the nation's critical infrastructures. It is also envisioned that each group will seek additional funding support through grant and sponsorship activities as appropriate to facilitate research and deliverable objectives.

Critical Analysis *(continued from Page 2)* Across the United States and within cities, much of the networked infrastructure (rail, highway, telecommunications, and pipelines) is located along shared rights-of-way. Rail, highway and maritime transport systems coincide at intermodal facilities and transshipment points.

Because of the way critical infrastructure is spatially arranged and interconnected, a disruption to one part of one network can have negative ripple effects on the performance of other networks, according to Homer-Dixon. The points in this infrastructure where vulnerabilities are the greatest are what he calls "weak links." In telecommunications circles, the classic example of such a link is New York City's 60 Hudson Street and 111 8th Avenue in New York City, buildings that if destroyed would cut off over 80% of the Internet connectivity between the United States and Europe. Last July in Baltimore, there was an explosion in a tunnel that disrupted not only rail traffic up and down the east coast but also caused a substantial degradation in Internet connectivity in the Northeast as a result of key net cables along the right-of-way being melted. Here is another example of a "weak link" and the criticality of such a link.

Surprisingly, Homer-Dixon makes no mention of financial and banking services, and the "weak links" that exist in this infrastructure stemming largely from the sector's dependence on telecommunications, phone and transportation networks. In New York City, 3.5 trillion dollars of financial transactions run over high-speed phone *(Continued, Page 7)*

Chubb Group of Insurance Companies
Private Sector Participation in the Administration's
National Strategy to Secure Cyberspace

Global property-casualty insurance carrier Chubb is very pleased to have been invited to participate in crafting the *National Strategy to Secure Cyberspace*. Working side-by-side with Richard Clarke, Special Advisor to the President for Cyberspace Security, and a team from the Office of Homeland Security, Chubb is helping to underscore, and reinforce, the power of the public-private partnership to address the crucial issue of cybersecurity.

Chubb Chairman & CEO, Dean O'Hare, who met with Clarke and others in June to discuss the role that the insurance industry could play in support of the Office of Cyberspace Security's mission, believes that "today, protecting a company's cyber assets is as critical as protecting its physical assets. Computer technology has made us all interdependent – which has created incredible opportunities for growth. Unfortunately," O'Hare notes, "it's also created some incredible vulnerabilities."

At the meeting with the Homeland Security team, O'Hare explained that, "companies rely on vendors, IT suppliers, utilities, financial institutions and others in the 'supply chain' – all of which communicate with each other via the Internet – to conduct their business activities. If a terrorist attack, or *any* catastrophic event – whether 'physical' or 'cyber' – disrupts this chain, the resulting cascading failure could bring a company, an industry and, ultimately, the economy, to its knees. While insurance for some of these new vulnerabilities can certainly help minimize the financial impact of a cyber event," he said, "the better solution is a comprehensive loss prevention and business recovery protocol – a roadmap, if you will – for managing risks enterprise-wide that critical infrastructure industries can follow. That's why the President's Plan is such an important and necessary project."

Chubb has a long-established reputation as a leading provider of innovative insurance and risk transfer solutions for both personal and commercial customers worldwide. Over the years, the company has honed its expertise responding to the emerging property and liability insurance needs of an array of critical infrastructure industries including banking/finance, marine/cargo, health care, high tech, telecommunications and energy. For more information about Chubb, visit www.chubb.com

Critical Analysis *(continued from Page 6)* lines converging at ten data processing centers nationwide. Some experts have estimated that if the right phone lines were severed, the U.S. economy would shut down for an indefinite period of time and to make matters worse there is no evidence that a backup system is in place to handle such a catastrophe. The events of 9/11 revealed the following vulnerabilities: lack of geographic diversity, backup plans developed did not consider that transportation may be impaired, the telecommunications and power infrastructure was extremely fragile with no backup networks and a number of choke points or "weak links" exist where high levels of economic transaction occur (e.g., the Automated Clearing House Network, Fedwire and CHIPS.

The structural topology and complexity of networks is another source of vulnerability for developed nations, according to Homer-Dixon. Over *(Continued, Page 8)*

Critical Analysis *(continued from Page 7)* time, telecommunications and transportation networks have become much larger and increasingly complex in terms of their spatial properties making them unstable and more susceptible to cascading failures if attacked. This is because large, complex networks tend to be scale-free, meaning they have many nodes with just a few link attachments, and a small but significant minority that have multiple links. There are many examples of scale-free networks documented in the literature – the inter-metropolitan highway network for the United States, the airline hub-and-spoke system, and there is some research that suggests that the backbone for the Internet also falls into this category as well. One of the implications of scale free networks is that they deteriorate rapidly when nodes are strategically attacked. The Notre Dame Center on Self Organizing Networks found this out by experimenting with the removal of nodes in scale-free networks. They discovered that when nodes are randomly removed, the network does not become disconnected until over 80% of the nodes are removed. On the other hand, when the most connected nodes are removed the diameter of the network, a measure of connectivity, increases dramatically, doubling its original value if the top 5% are removed.

The silver lining in this is that in order to cause any major disruptions, the terrorist must target the "right nodes in the right network. " While for transportation networks critical nodes can fairly easily be identified through the use of a road map, information on traffic flows and a little bit of computing power, identifying these nodes in other networks poses some challenges. In the case of telecommunications networks for example, there is no single map showing how the networks of individual ISPs are actually interconnected through peering arrangements or a publicly available database of Internet traffic flow through the integrated system of networks. Accurately identifying critical nodes in the financial and banking services infrastructure is also difficult. To do this would require access to proprietary or sensitive data on the flow of information and money within the sector and to and from other firms, government entities and consumers. In addition, data on which Internet Service Providers and phone companies are used by each institution would also be important. Despite these difficulties, there is always the possibility that a terrorist can gain access to critical information by hacking into a computer, and this threat should not be ignored.

While Homer-Dixon provides a compelling set of arguments on just how vulnerable the developed world is to terrorism, and to acts that can have crippling effects and cascading failures, he falls short in offering solutions to the problem. He mentions a few strategies – i.e., loosening the couplings and unstable properties of economic and technological networks by utilizing "circuit breakers" that stop cascading failures and dangerous feedback loops, and dispersing critical assets. The discussion of these solutions lacks in any depth. Practical issues related to the implementation of these strategies are not addressed. First, the strategies presented by Homer-Dixon all imply losses in economic efficiency, as he notes, yet it is not clear as to how this problem can be circumvented. Over time, the market has clearly demonstrated that there are powerful gains in economic efficiency by integrating networks and clustering activities, and the location behavior of many firms is largely driven by this reality. Certainly, it is true that future terrorist attacks could increase rents and insurance premiums in vulnerable locations, or create a "fear factor" prompting some firms to naturally disperse, but the benefits of agglomeration will most likely prevent any substantial deconcentration of activity. Homer-Dixon does not address how economic barriers like this will be overcome. Will it be necessary to offer economic incentives to firms to relocate in low-density areas or should the government intervene through regulations in the interest of national security? Second, relaxing the interdependency between networks and the coupling effects that have evolved in this structure requires careful coordination between a variety of institutions and firms. Building redundancy into the telecommunications network for example, will require individual ISPs to work together and share critical information to establish peering arrangements and alternative routes.

Homer-Dixon's discussion of solutions also falls short in that he neglects to consider a very important set of solutions – i.e., those that are technology-based. While the process of technological development has clearly contributed to the vulnerability of modern society to terrorism, as
(Continued, Page 9)

Critical Analysis *(continued from Page 8)* he clearly describes in the paper, Homer-Dixon fails to acknowledge that technology can also serve as a "weapon of defense." There are ample examples of where technology can play a pivotal role in promoting national security. In many metropolitan areas, transponders on buses are used to track the movement of these vehicles and to promote the safety and security of drivers and passengers. The same technology could be applied to containers carrying hazardous materials. A satellite-based communication system linking major banks with funds transfer and clearance centers could be used in the chance of a catastrophic power or telecommunications failure. Technology and technical knowledge can also be used to build redundancy into our telecommunications networks and in fact this is already being done by certain ISPs. Sprint's backbone network has duplicate links between nodes, where each pair is designed so that no single link carries more than half of the network's traffic. In the Baltimore tunnel fire, this system proved effective in mitigating reductions in customer service. Lastly, we even have the computing power and technical skills to run simulations of different attack scenarios and to test various plans!

There are still a lot of unanswered questions and a need for further research and development in this area. In particular, we need to gain a better understanding of the topology and structure of critical infrastructure. The questions are endless. What cities are most "critical" to the telecommunications network, playing a pivotal role in receiving and disseminating information via the Internet? Where are the "critical" nodes and links located in these networks? How do the networks interface with financial and banking services? Is the geographic dispersion of information, financial and banking infrastructure a desirable tactic for minimizing the negative implications of a targeted attack on key facilities in either city? If so, how should these facilities be spatially distributed? What types of services are provided by the banking and financial sector? What is the relative importance of these activities and the flow of information from various institutions? How would the connectivity and performance of the Internet be affected by the removal of "critical" cities from the network resulting from a physical attack on some key infrastructure facilities, e.g., a collocation facility or metropolitan area exchange (MAE) for example? How would coordinated fiber cuts to multiple links impact the network's performance and connectivity? What cities should be identified as backup nodes in the event of an attack and how should traffic be rerouted? What is the importance of interconnection agreements in mitigating catastrophic and cascading effects resulting from a targeted attack? Should incentives be offered or regulations put in place to facilitate cooperation between ISPs?

Only by trying to understand this can we begin to formulate plans and policies designed to mitigate the catastrophic and cascading effects that could occur as the result of a targeted physical and/or cyber attack on infrastructure in the developed world. And we need to understand our complex infrastructure even better than the enemy. This is recognized by Homer-Dixon: "Terrorists have significant leverage to hurt us. Their capacity to exploit this leverage depends on their ability to understand complex systems that we depend on so critically. Our capacity to defend ourselves depends on that same understanding."

Citations:

Albert, R., Jeong, H. and Barabási, A.L. (2000) Attack and error tolerance in complex networks. *Nature* 406**:** 378

McKinsey and Company (2001) Impact of Attack on New York Financial Services. *The McKinsey Quarterly.*

Hopkins, J. (2001) Electronic financial networks: How safe are they?. *USA Today.*

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

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