MAY 2004 / VOLUME 2, NUMBER 11

THE CIP REPORT

Special Issue: International CIP

CIP Project Staff

John McCarthy, *Executive Director*

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

Rod Nydam, *Associate Director, Private Sector Programs*

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

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

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

Contact: cipp01@gmu.edu
703.993.4840

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

Message from John McCarthy, Director of the CIP Project:

This Special Issue of *The CIP Report* is focused on critical infrastructure protection (CIP) from an international perspective. It is important to address CIP from a global viewpoint because infrastructures are shared among many nations and what happens in one country has cascading effects on critical services in another. Furthermore, we may also collectively learn from the activities, initiatives, and insights of professionals around the world who are addressing daily challenges in protecting their critical infrastructures through the lens of their unique cultures and legal, political and technical frameworks.

As a participant in the recent CIP bilateral meetings between the U.S. and Australia, I observed collaboration between government officials, private sector actors and academia. I was reminded of the absolute value of this type of effort and the need to further this important dialogue on protecting global assets.

In this issue, you will find information about what is taking place in different countries--legislatively, politically, and technically--with regard to CIP as well as varied perspectives on its inherent challenges. Many voices are represented in order to provide an overview of a range of efforts underway. We look closely at what the United States government is doing on multiple levels and include several thought pieces on international issues. Although this is our biggest issue yet, we only touch on a fraction of the initiatives, nations, and individuals involved in the critical infrastructure protection arena.

The CIP Project has concentrated largely on domestic CIP issues, but we hope this initial foray into the international realm will provide a foundation for additional attention and focus.

THE TECH CENTER
National Center for Technology & Law

CRITICAL INFRASTRUCTURE PROTECTION PROJECT

AUSTRALIA

CIP Policy Down Under

Trevor Clement
Assistant Secretary, Critical Infrastructure Protection
Australia

The Australian Government's policy for critical infrastructure protection (CIP) seeks to ensure there are adequate levels of protective security for critical infrastructure, minimum single points of failure, and rapid, tested recovery arrangements. The national approach to CIP in Australia is articulated through the National CIP Strategy, which defines critical infrastructure as follows:

Those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic well-being of the nation, or affect Australia's ability to conduct national defence and ensure national security.

The Australian delegation at the April 2004 CIP Bilateral Talks with the United States

The Australian Government has taken an "all hazards" approach to CIP. Critical infrastructure can be damaged, destroyed or disrupted by natural disasters, negligence, accidents or by deliberate acts of terrorism, computer hacking, criminal activity and malicious damage. While terrorism has assumed a higher profile in Australia's current threat environment, our critical infrastructure has to be protected against all threats and hazards presenting a risk to the continuity of service.

The Australian Government's CIP policy has three key objectives:

1. enhancing the identification of critical infrastructure and determination of risks;
2. mitigating risks to critical infrastructure; and
3. refining, enhancing and promoting CIP best practice.

It has been recognised in Australia that since the majority of critical infrastructure is privately owned and operated a strong business-government relationship is essential for Australia to effectively respond to any threats to critical infrastructure. Thus the main vehicle through which CIP is affected in Australia is a network of Australian governments and critical infrastructure owners and operators known as the Trusted Information Sharing Network (TISN). This body was created to enable the owners and operators of Australia's national critical infrastructure to share information and develop strategies to mitigate risk to critical infrastructure. The TISN is intended to allow the owners and operators of critical infrastructure to share information on important issues such as business continuity, consequence management, information system attacks and vulnerabilities, e-crime, protection of key sites from attack or sabotage.

The TISN includes a number of groups for different critical infrastructure sectors, known as Infrastructure Assurance Advisory Groups (IAAGs), which comprise representatives from across the respective industry sectors. Each of the IAAGs also includes an Australian Government representative. Groups for the banking and finance, communications, energy, food chain, emergency services, health and water services sectors are well established. Additional IAAGs for Iconic & Public Buildings (*Continued, Page 3*)

Australia (*Cont. from Page 2*) and Transport will be formed in the third quarter of 2004.

The Critical Infrastructure Advisory Council (CIAC) also forms part of the TISN. It oversees the IAAGs and provides advice to the Attorney-General on the national approach to protecting critical infrastructure. The CIAC consists of representatives from each of the critical infrastructure business sectors, each of the Australian States and Territories, relevant Australian (federal) Government agencies and the National Counter-Terrorism Committee. The CIAC concentrates on the medium-to-long-term issues concerned with the prevention, preparedness and recovery aspects of CIP, particularly those matters requiring coordination with the private sector. The CIAC also assists in identifying research issues requiring priority attention.

Although the TISN is the main conduit between industry and government on CIP issues, and the National CIP strategy has a deliberately "all hazards" focus, it is clear that in the current threat environment particular attention needs to be paid to terrorism. In response to this awareness CIP work is also being undertaken by Australia's National Counter-Terrorism Committee (NCTC).

Australian Governments and industry have recognised and agreed to develop some immediate measures and procedures to counter the heightened threat of terrorism to critical infrastructure. The NCTC has been tasked to work with governments and industry to address this issue. The role of the NCTC in CIP is to ensure a national strategy is developed and maintained for the coordination of the protection of critical infrastructure from terrorism. This is reflected in Australia's National Counter Terrorism Plan and National Counter Terrorism Handbook. The NCTC will include CIP as a theme in counter terrorism training and exercises, and will consider specialist capabilities for responders to work in and around critical infrastructure.

The U.S. delegation at the bilateral talks

The lead agency for national CIP policy in Australia is the federal government's Attorney General's Department (AGD). This agency, and in particular it's Critical Infrastructure Protection Branch, has the primary strategic and coordination role for national CIP policy. The Protective Security Coordination Branch of AGD, at the direction of the NCTC has responsibility for the counterterrorism aspects of national CIP policy.

AGD has recently received new funding for the expansion of its overall CIP program. Three main outcomes of this new funding include an increased support for the TISN; the development of a modelling and analysis capability for critical infrastructure interdependencies; and the development of a network security vulnerability analysis capability. These and other projects will ensure that the CIP groundwork already established in Australia can be constructively expanded upon in the coming years to effectively protect Australia's national critical infrastructure from a wide variety of threats.

In summary, Australian national CIP policy is a coordinated approach that revolves around a dense network of many Australian (federal) Government agencies, all the State and Territory governments and critical infrastructure industry sectors. Many of the institutions of Australian CIP are still in their formative stages, although strong inroads have been made in many areas. The recent increased funding for national CIP will ensure that the networks and projects essential for the effective protection of Australia's critical infrastructure can be established without delay. Further information about Australia's national CIP policy can be obtained at www.tisn.gov.au. ❖

CANADA

Canada Releases National Security Policy

In April 2004, Canada's Deputy Prime Minister released a strategic framework and action plan for facing current and future threats entitled "*Securing an Open Society: Canada's National Security Policy*."

The National Security Policy focuses on addressing three core national security interests:

- protecting Canada and Canadians at home and abroad;
- ensuring Canada is not a base for threats to its allies; and
- contributing to international security.

The policy contains several measures that will contribute to an integrated security system, including an Integrated Threat Assessment Centre to serve as a collection and dissemination point for threat-related information, a National Security Advisory Council consisting of non-governmental security experts, a Cross-Cultural Roundtable on Security, and build on the newly created Department of Public Safety and Emergency Preparedness.

The new policy focuses on six key strategic areas, including intelligence, emergency planning and management, public health, transport security, border security, and international security. The policy examines each of these areas acknowledging accomplishments already made, addressing security gaps, and identifying key measures to be taken.

Critical infrastructure protection is addressed in the emergency planning and management section of the policy document.

Context

Canada's current approach to emergencies dates back to the Cold War era. The system is based on a highly decentralized and distributed division of responsibilities among first line responders, provinces and territories, and lead departments at the federal level. There is currently an urgent need for a more modern, integrated national support system for first line responders, and there remains a system-wide question about the adequacy and sufficiency of resources for key players across the country, particularly in the context of sustained and operationally intense emergency situations. Interoperability of policies, systems and personnel is also a major national challenge that must be tackled. And there is undoubtedly a need for clear national leadership - both on the ground and in communications - on emergencies of national importance.

Effective emergency management comprises several phases, including mitigation, prevention, preparedness, detection, response, recovery, and evaluation. In all of these phases, national capacity must be bolstered, and policies and operations made seamless across jurisdictions. In saying this, the Government of Canada recognizes that first line responders lie at the heart of the emergency management system and that the federal Government will often play only a supporting role in emergency management to provinces and territories, communities and the private sector. The Government has identified two important elements for modernizing Canada's approach to emergency management:

- first, building on key measures taken to date, the Government will put its house in order by launching initiatives to fill the highest-priority gaps; and
- second, the Government will, in concert with its partners in the provinces and territories, and drawing on communities, first line responders and industry, launch a process to determine how to collectively modernize the national system of emergency management.

Progress to Date

Since September 11, 2001, the

(*Continued, Page 5*)

Anne McLellan
Deputy Prime Minister
and Minister of Public Safety and
Emergency Preparedness

"While there is no indication of any specific, imminent threat to Canada, it is important that we remain vigilant and work closely with our international partners, particularly the U.S., to keep Canadians and our allies safe. The National Security Policy highlights the risks to Canada and presents a coordinated strategy for managing and responding to these risks."

Canada (*Cont. from Page 4*)
Government has taken steps to bolster its performance and capacity to effectively manage complex emergencies:

- It increased resources for dealing with chemical, biological, radiological or nuclear attacks (CBRN) including networked federal laboratories for research, the development of a four-level training program for first line responders and the accelerated delivery of new technologies to first line responders through the CBRN Research and Technology Initiative.
- It implemented the National Urban Search and Rescue program to build and enhance the capabilities of first line responders to respond to emergencies resulting in structural collapses.
- It enhanced the ability of law enforcement agencies to investigate cyber-incidents and other threats to national security.
- It enhanced federal-provincial-territorial co-operation on emergencies, including major exercises.
- It created a new Government of Canada standard for maintaining government operations during emergencies.

The Way Forward

Building on the measures taken to date, the Government will take immediate steps to put the federal house in order by addressing the highest-priority gaps in its capacity to manage emergencies in the areas of overall strategic co-ordination, critical infrastructure protection and cyber-security. Canada is committing an additional $105 million to address these gaps.

Strategic Coordination

The Government will build a centralized Government Operations Center to provide stable, round-the-clock coordination and support across government and to key national players in the event of national emergencies. The Operations Center will be housed in the Department of Public Safety and Emergency Preparedness, and will provide leadership in emergencies of national importance.

A seamless national emergency management system requires a comprehensive, modern legislative foundation, informed by consultations with provinces, territories, communities, first line responders, and industry. To this end, the overall statutory framework for the Government's emergency management activities - in particular the *Emergency Preparedness Act* - will be reviewed and modernized to reflect the emerging requirements of emergency management. These requirements cover the areas of mitigation programs, critical infrastructure protection, cyber-security, information-sharing between federal departments, agreements with international and private sector partners, and protection of sensitive private sector information.

Recent events in Canada such as SARS have called into question the effectiveness of existing disaster financial assistance arrangements to deal quickly and effectively with response and recovery. The need for consistency of application, improvement of federal-provincial-territorial cooperation, and a comprehensive federal response is driving the development of a framework for responsive disaster recovery assistance.

As part of this, the Government will complete an ongoing review of the Disaster Financial Assistance Arrangements, develop guiding principles for other federal instruments to complement these arrangements for situations such as public health and animal health emergencies, and examine the inventory of existing national programs and
(*Continued, Page 32*)

EUROPEAN UNION

European Network and Information Security Agency

The European Network and Information Security Agency, ENISA, is a new agency of the European Union which formally came into being on 15 March 2004.

The Agency was set up to enhance the capability of the Community, the Member States and consequently the business community to prevent, address and respond to network and information security problems. In order to achieve this goal, ENISA will develop a high level of expertise and stimulate the cooperation between the public and private sectors.

In order to ensure the fulfillment of its objectives, the Agency's tasks will be focused on:

- First, advising and assisting the Commission and the Member States on information security and in addressing security-related problems in hardware and software products in their dialogue with industry.
- Secondly, collecting and analysing data on security incidents in Europe and emerging risks;
- Thirdly, promoting risk assessment and risk management methods to enhance our capability to deal with information security threats.

The Agency shall also assist the Commission in the technical preparatory work for updating and developing Community legislation in the field of network and information security. ❖

EU Overhauls Security and Response Programs After Madrid Bombing

In reaction to the railway bombings in Madrid on March 11, the European Union (EU) is consolidating a single, cross-European civil defense framework. An Action Plan released by the European Commission (EC) establishes new coordination mechanisms to assess threats, share threat data, and coordinate responses to terrorist attacks. The Europeans are preparing an all-hazards response plan to facilitate restoration and recovery after a terrorist event, which is similar to the US National Response Plan.

The EC proposes three actions, all of which mirror efforts within the United States:

1. Resource management: EU countries cannot fully prepare for contingencies individually. Member nations should provide detailed inventories of all resources; expertise then can be shared in the event of a disaster or attack.

2. Training: The EC proposes combined training and exercises among EU nations to allow them to work together more effectively.

EU R&D Strategy

European R&D strategy emphasizes security and may give a competitive edge to European companies: The Europeans are exploring a "community" approach to security research and development. In contrast to the U.S. strategy, which prioritizes countermeasures for weapons of mass destruction, the Europeans are pooling resources to prioritize cyber security, infrastructure assurance, and incident management.

3. Financing: The EC recommends more funding to cover transportation and other costs incurred after a disaster. ❖

JAPAN

Japan Focuses on IT Security with New Initiatives

The Japanese government has updated its IT policy framework for strengthening e-government in Japan. The Cabinet Office released the Acceleration Package for the e-Japan Strategy in March to advance the country's IT strategy. In a separate document, a government working group outlined a series of privacy guidelines for companies that use radio frequency identification devices. The Japanese government hopes to achieve full operational implementation by 2005.

The acceleration package focuses heavily on the following security initiatives:

- Critical infrastructure:
Recognizing that information technology underlies the stability of Japan's critical infrastructures, the package calls for cooperation between the public and private sectors to establish IT technical and operational standards.

- Government security:
The package calls for the creation of an information security officer position in the Cabinet Office to promote information security policy in government and industry.

- Credentialing:
The government intends to issue ID cards to its employees that will be standardized and increase security.

- Information sharing:
The creation of an information sharing system for use during disasters would facilitate communication with the government and between the public and private spheres. ❖

Japan Releases Government IT Vulnerability Assessment

The Japanese government recently completed a security survey of IT vulnerabilities in government agencies, which found many critical systems vulnerable to Internet attacks. The Cabinet Office, which is similar to the White House Office of Management and Budget (OMB), conducted the cyber-security survey. The National Police Agency and the Japanese Defense Agency assisted in the IT vulnerability assessment.

- Of the agencies and ministries inspected, the Cabinet Office discovered more than 153 "high risk vulnerabilities," which cover critical systems susceptible to attacks launched from the Internet and from within the ministries by insiders. The Japanese press also reported that the study discovered 633 "moderate-risk" vulnerabilities.

- According to the Cabinet Secretariat, the level of information security within and between ministries varies greatly. The Secretariat plans to notify each ministry about the security gaps, but the ministries themselves will take remedial action.

The Cabinet Secretariat will conduct a follow-up survey and begin drafting information security standards, which are expected to be similar to the guidelines produced by the OMB and the National Institute of Standards and Technology in the US. ❖

SWEDEN

CIP in Sweden: Network-based crisis management system

Jan Lundberg, Strategic Analyst
Swedish Emergency Management Agency
Information Assurance and Analysis Department

Networks are needed to handle the threats, risks and vulnerabilities of our information and networked society.

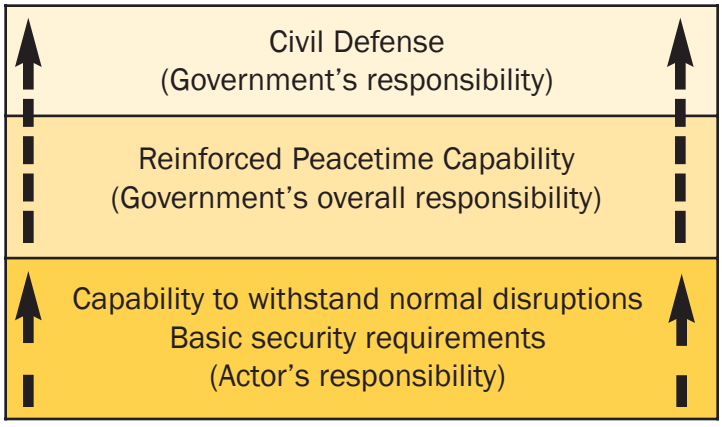
Jan Lundberg

Protecting critical infrastructure is high on the Swedish agenda. A new crisis management system was created on July 1, 2002 to strengthen the proactive and reactive crisis management capabilities of our society. The Swedish Emergency Management Agency (SEMA) was tasked with co-ordinating society's work with emergency preparedness. One of the most important tasks is critical infrastructure protection (CIP).

Six cooperation areas were formed to strengthen collaboration between the most important authorities and players within each area, and to avoid "stovepipe" problems. One of the most important tasks for players in each area is to strengthen the protection of the critical infrastructure. SEMA also has overall responsibility for society's information security. One of the most important features of the Agency's work is cooperation with the private sector.

During the Cold War, the most important national security issue was losing territorial control over the country. The most important issue today is losing functional control over the country and its infrastructures. A functional map of important operations and services, their mutual dependencies and vulnerabilities is currently under construction. One of SEMA's most important tasks is to create and maintain an overview of threats, risks and vulnerabilities.

Critical infrastructure in Sweden, as in the United States, is owned and operated by private companies. Deregulation has led to security problems and breakdowns. SEMA proposes that the Government makes new demands on secure infrastructure operation. The conditions are illustrated below.



During the Cold War, Sweden bordered East Germany and the Warsaw Pact in the south, and the USSR in the north. A strategic assault on the country was an assumed risk during the 1980s. The sabotage of infrastructure and government was considered a major risk in any attack. Thus, protecting the critical infrastructure has long been an issue in Sweden.

The Swedish defence policy was based on the concept of Total Defence, i.e. that war affects the whole society. War was total, and all available civilian and military resources had to be be able to mobilise and co-operate to withstand its effects. The private sector was a vital part of Total Defence. Civil preparedness was created by ensuring that peacetime society had the strength, resources and resilience to manage the consequences of peacetime emergencies. Additional emergency preparedness measures were taken to prepare for serious crises or war. An important principle was that peacetime society should not be unnecessarily vulnerable.

The risk for a major war in Europe is no longer present, nor the need for Total Defence. But the experience of physically protecting the critical infrastructure and building (*Continued, Page 11*)

Public Private Partnership and the Provision of Societal Security

Jan Joel Andersson and Andreas Malm
4C Strategies AB, Sweden

National Defense is the sole responsibility of the government, but who is responsible for "Homeland Defense" and societal security? In a non-liberalized economy, the state assumes both the responsibility as well as the costs of guaranteeing critical infrastructure systems and services to ensure societal security and public safety. It is more problematic assigning a clear responsibility for securing such systems and services in a liberalized economy where the majority of critical infrastructures is in private hands. Given the importance of the private sector in providing societal security and emergency management it is paramount to establish where and when private sector responsibility for societal security and public safety ends, and where and when government responsibility begins.

Market forces do provide some incentives to firms to avoid the direct financial costs of disruption of their operations due to crises and unforeseen events. However, in general, market incentives are not compelling enough for private actors to provide the appropriate level of security for society as a whole. To survive in a market driven economy, companies need to minimize costs. Keeping reserve stock, maintaining redundant systems, and employing back-up staff all cost money. With pressure to cut costs less resources are available for contingencies and crisis management. Bankruptcy laws and moral hazard further limits the extent to which private actors are willing to extend their emergency preparedness and crisis management capabilities.

The diminishing role of the state in the provision of essential services, such as energy, communications, and financial services, in combination with private companies need to minimize costs lead to a situation that we describe as a gap between government emergency preparedness measures (which, of course, varies across sectors), and private actors' lack of interest in providing sufficient such measures for society as a whole. This gap is illustrated in figure 1 below.

The gap between government and private actors' emergency preparedness measures indicates that market incentives are not enough to provide sufficient societal security. Since the market is unlikely to close the gap by itself, the government must "help the market work" by altering the incentive structures to close the gap.[1] While market forces are potent, one must remember that over-reliance on markets is just as dangerous as over-reliance on the powers of direct regulations.

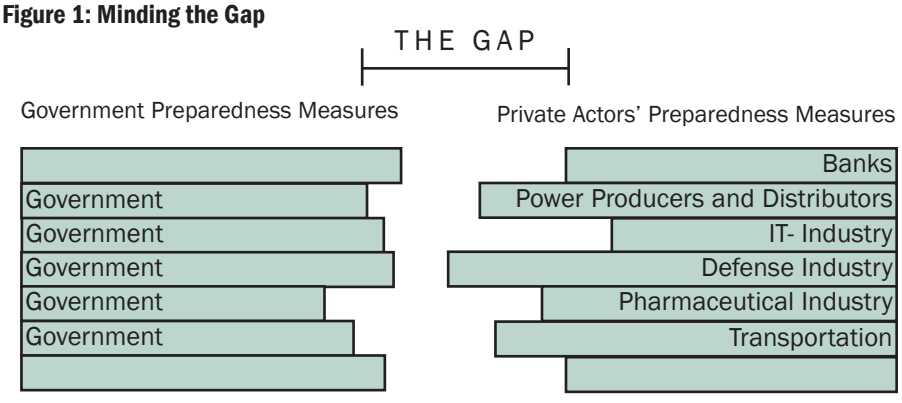
Closing the Gap

In principle, there are three ways in which the gap in emergency preparedness between public and private actors could be closed. The first alternative is legislative regulation, the second alternative is to use economic policy instruments, and finally, the third alternative is to turn to Public-Private Partnerships. We will discuss each alternative in turn but focus our discussion on Public-Private Partnerships.[2]

Direct Regulation

The argument for regulation is that it will provide a uniform level of emergency preparedness (assuming that the regulations are followed and enforced)
(*Continued, Page 29*)

Figure 1: Minding the Gap



Source: Jan Joel Andersson and Andreas Malm. "Minding the Gap: Reconciling Responsibilities and Costs in the Provision of Societal Security", paper presented at the conference on Societal Security and Crisis Management in the 21st Century - 6th CRN International Expert Workshop, Stockholm, April 23, 2004. Available at http://www.isn.ethz.ch/crn/_docs/Andersson_Malm.pdf

SWITZERLAND

Towards an International Regime for the Protection of Cyberspace?

Myriam Dunn, CIIP Research Group, Center for Security Studies
ETH Zurich (Swiss Federal Institute of Technology), Switzerland

Like other security issues, the vulnerability of modern societies caused by dependency on a spectrum of highly interdependent information systems has global origins and implications. To begin with, a variety of malicious actors in the cyber environment are willing to contravene national legal frameworks and hide in the relative anonymity of cyberspace. Further, the information infrastructure transcends territorial boundaries so that information assets vital to the national security and the essential functioning of the economy of one state may reside outside its sphere of influence on the territory of other nation-states. Additionally, cyberspace - a huge, tangled, diverse, and literally universal blanket of electronic interchange - exists everywhere where there are telephone wires, cables, computers, or electromagnetic waves, a fact that severely curtails the ability of states to regulate or control it alone. Any adequate protection policy extending to strategically important information infrastructures will thus ultimately require transnational solutions, such as an international regulatory regime for the protection of cyberspace.

Regulatory regimes[1] emerge from the mediation of disparate interests of various stakeholders within arenas of political interaction. The outcome of these interactions usually takes the form of new rules, which are created by constraining actors' choices and pre-scribing who can act when, and affect behavior both directly and indirectly. But even though the need for such an international regime in the area of information security or critical information infrastructure protection (CIIP) is evident, there are at least two problems delaying its emergence.

First, CIIP is an issue of high relevance to many different, very diverse, and often over-lapping communities. These different groups - be they private, public, or a mixture of both - do not often agree on what needs to be protected with what means. In addition, turf battles within governments are frequent; only in a few countries have central governmental organizations been created to deal specifically with CIIP issues. Often, responsibility is given to well-established governmental organizations or agencies that appear suitable for the task.[2] Depending on their key assignment, these agencies bring their own perspective to bear on the problem and shape policy outcomes accordingly.

As a result of both points, the difference in the scope and quality of national CIIP policies is considerable. CIIP policies in various countries are at various stages of imple-mentation - some are enforced, while others are just a set of suggestions - and come in various shapes, ranging from a regulatory policy focus concerned with the smooth and routine operation of infrastructures and questions such as privacy or standards, to the inclusion of CIIP into more general counterterrorism efforts. This divergence of national CIIP policies is a major obstruction to the development of an international regime, for international regimes are based on at least a minimal convergence of expectations and interests of (national) key actors.

Second, there exists a paradoxical desire of many NATO states to both exploit and restrict attacks against the information infrastructure simultaneously. Under the broad heading of "Information Operations" they seek to integrate attacks against the information infrastructure of a foreign state into routine

(*Continued, Page 11*)

Dunn (*Cont. from Page 10*) military planning as a tool of strategic coercion, while at the same time, they take a range of actions, both unilaterally and multilaterally, to mitigate the risks resulting from the dependency of their own militaries, governments, economies, and societies on networked information systems.

The problem with these military ideas for the strategic use of cyberspace is that they fail to recognize the nature of the (emerging) interdependent network environment, which will likely be characterized by ubiquitous computing and networking - and thus even greater interdependencies. This fact makes it unlikely that computer attacks can ever be a tool for precise targeting of enemy infrastructures or a means to deliver effectively to a particular geographic conflict zone. In fact, not only could military use of computer attacks directly "blowback" on Western societies through the network interdependencies; routine use of computer attacks would also likely result in a more intangible side effect: the undermining of trust in cyberspace with long-term effects on the global economy. This basically means that the investments in military technologies and doctrines designed to disrupt the infrastructures of rival nations seem like a comparative strategic advantage only at a first glance: A closer look will reveal that these benefits are considerably flawed by misperceptions of the emerging technical environment and the nature of the international system in the information age in general.[3]

The problems outlined above are two main factors slowing down the emergence of norms for the protection of cyberspace. However, in the light of economic and security interests, industrialized states would be well-informed to work towards overcoming these temporary obstacles and move resolutely towards robust international conventions and mechanisms that protect the global information environment.

[1] A regime can be defined as "sets of implicit or explicit principles, norms, rules, and decision-making procedures around which actors' expectations converge in a given area of interna-tional relations". See: Krasner, Stephen D. (ed.). International Regimes. (Ithaca: Cornell University Press, 1984): p. 2.

[2] Dunn, Myriam and Isabelle Wigert. The International CIIP Handbook 2004: An Inventory of Protection Policies. (Zurich: Center for Security Studies, 2004).

[3] Rathmell, Andrew. "Controlling Computer Network Operations". In: Wenger, Andreas (ed.). The Internet and the Changing Face of International Relations and Security. Information & Security: An International Journal, Volume 7 (2001): pp. 121-144 ❖

Sweden (*Cont. from Page 8*) a robust peacetime society is still valuable. Especially with regard to the cooperation that took place within the Total Defence framework. Most Swedish adults were involved in Total Defence in some way. Redundancy and reserve systems were incorporated into important infrastructure systems such as the electricity supply, telecommunications, water supplies, data systems, etc.

A Total Defence system though had to be a planned system, as most defence forces. The challenge now is to build a Risk Management based system with short OODA (observe, orient, decide, act) decision loops. New threats, risks and vulnerabilities must be addressed in time. This demands new methods and changing the mind sets of those used to the old Total Defence concept, while not losing the lessons learned in cooperation and CIP.

SWEDISH EMERGENCY MANAGEMENT AGENCY

Sweden's security policy situation has now undergone a fundamental change. The country, itself an EU member, is surrounded by democratic states that are members of the EU, NATO or both. Russia does not constitute a military threat to Sweden.
Our world has become more secure but less predictable. History has not ended; international terrorism and organized crime constitute the new threats. Open borders, interconnected infrastructure systems and the rapid expansion of electronic information services create new vulnerabilities. The challenges can only be solved by co-operation: nationally, within the EU and in other international fora. The transatlantic cooperation is an import part of successful CIP.

For more information: www.krisberedskapsmyndigheten.se and www.isn.ethz.ch/crn ❖

UNITED KINGDOM

Civil Contingencies Bill Released by UK Government

The UK Cabinet Office has published a final draft of the Civil Contingencies Bill, which is intended to "deliver a single framework for civil protection in the UK." Like the Homeland Security Act of 2002 adopted in the US, the UK law modernizes civil preparedness responsibilities and organizations. Unlike the approach taken in the US, however, the UK government is not creating a new department or consolidated agency to address evolving security challenges.

The UK bill is vastly different than homeland security policies adopted by Congress and the Administration in two areas.

- First, the Civil Contingencies Bill, if adopted, would impose significant duties of care on infrastructure owners. Category 2 Responders (refer to chart below), which principally include infrastructure utilities, must undertake seven areas of security preparedness, such as performing risk assessments, developing plans, and training. In addition, infrastructure providers must share information with local responders and collaborate during security emergencies. Since publication of the draft Civil Contingencies Bill last year, the UK government has narrowed the list of critical infrastructure sectors that will be directly affected. The UK government includes a "duty to warn," but the duty is limited to Category 1 Responders, which are primarily government entities.

- Second, the UK bill focuses principally on resilience at the local level. Like Congress and the Bush Administration, UK government officials are struggling to balance local, regional, and national solutions. In defining roles and responsibilities the UK bill delegates significant authority to local administrators, rather than regional or national responders and government entities. National resilience, the UK government concludes, will follow from local preparedness and response capabilities.

Category 1 Responders	Category 2 Responders
County, Metropolitan, and Borough Councils	Electricity Suppliers
Unitary and State District Councils	Gas Suppliers
Police Forces	Water Undertakers
Fire Authorities	Telecommunications Operators
Ambulance Authorities	Railway Operators
Trusts	Airports
Environment Agency	Ports and Harbors
Maritime and Coastguard Agency	Health and Safety Executive

The UK government also has published an extensive cost-benefit analysis of the final bill. According to this analysis, active intervention by the government, which in this case involves requirements to enhance business resilience, can significantly reduce business risks. According to the World Bank and the US Geological Survey, the cost-benefit analysis concludes, economic losses worldwide in the 1990s could have been reduced by $280 billion if $40 billion had been spent on preparedness, mitigation, and prevention strategies.

A Regulatory Impact Assessment, model regulations, a report on the results of a 12-week public consultation, and the UK government's responses to pre-legislative scrutiny accompany the Civil Contingencies Bill, which can be viewed at http://www.ukresilience.info/ccbill/ ❖

Building an International Critical Infrastructure Protection Policy

Globalization brings tremendous benefits to individuals, businesses, and governments worldwide. Yet, as this process increases our interdependencies, it simultaneously increases our vulnerabilities, as links between U.S. and foreign critical infrastructures deepen. Prior to 9/11, the challenge of protecting critical infrastructure remained largely theoretical despite persistent attacks against information infrastructures. Today, more than ever, we recognize the necessity of international cooperation in securing our infrastructures, as we are only as strong as the weakest link.

The goal of international CIP policy, therefore, is to shape the international environment to reduce the risk to critical U.S. and foreign national information and physical infrastructures on which the U.S. and its allies depend for their national security and economic well-being. The U.S. Department of State, in conjunction with the Department of Homeland Security and other interagency partners, coordinates federal efforts to enhance international cooperation on critical infrastructure protection.

The CIP policy and outreach program is based in the Office of Plans, Policy, and Analysis in the Bureau of Political-Military Affairs, and guided by Michele Markoff, Senior Coordinator for International Critical Infrastructure Protection Policy. For cyber infrastructures, the program proceeds from the conviction that the U.S. cannot guarantee the reliability, availability and integrity of its information infrastructure if the foreign infrastructures to which it is inextricably linked are not secure. For physical infrastructures, this program is predicated on the fact that the U.S. depends heavily on specific allied and other physical infrastructures for force projection, forward military deployments and flows of goods.

This program has been implemented since 1998 under authorities that include PDD-63, E.O. 13231 (revised by E.O. 13286, March 1, 2003), the 2003 National Strategy to Secure Cyberspace and the associated National Strategy for the Physical Protection of Critical Infrastructure and Key Assets, and, most recently, HSPD-7 "Directive on Critical Infrastructure Identification, Prioritization, and Protection" (December 17, 2003).

The Department has chaired an International CIP Working Group since 1999 that consists of Departments and Agencies with international CIP goals, objectives and/or equities. Participants include the Departments of Homeland Security, Defense, Commerce, Justice, Energy, the National and Homeland Security Councils, and others. These meetings allow members to update one another on current activities and request assistance from colleagues as needed. Outreach initiatives are developed and conducted as an interagency process. The Department synthesizes interagency-specified goals and develops a foreign policy strategy designed to achieve them. Outreach activities also include the participation of senior U.S. industry representatives where their presence is likely to enhance the success of a particular mission.

Outreach is conducted across sectors in bilateral, multilateral and international fora to encourage nations to take systematic domestic and international steps to enhance the cyber and physical security of their critical infrastructures. Additionally, we maximize existing and long-standing relationships the various departments already have - bilaterally and multilaterally - whether within the Council of Europe, APEC, OECD, NATO, the UN, OAS, etc.

U.S. international CIP strategy consistently focuses on core themes reflecting the spectrum of interagency objectives. These themes are tailored to the specific country or region. If applicable, the (*Continued, Page 14*)

International CIP Policy (*Cont. from Page 13*) strategy identifies shared CIP interdependencies that need to be addressed to enhance U.S. security. The interagency process requires constant coordination, review, and revision. One does not craft an international strategy once and allow it to remain static. It changes over time based on the global environment, progress made, and changing priorities, among other factors. Currently, the Department is supporting the DHS-led effort to develop the first National Infrastructure Protection Plan by encouraging sectors to undertake efforts to map out their international interdependencies and then identify and prioritize countries for engagement in order to reduce the risk to these shared critical interdependencies.

The U.S. has held critical infrastructure protection bilaterals with nations that include Australia, Canada, Italy, India, Germany, Japan, and the Netherlands and had less formal discussions with the Republic of Korea and China. Multilateral efforts include the initiation of a regional cyber security strategy within the 34 Member Nations of the Organization of American States (OAS). In June, the OAS General Assembly will approve a resolution adopting this strategy that incorporates the modernization of laws governing the misuse of information technologies, the adoption of security standards, raising cybersecurity awareness and promoting education, and calling on all members that do not already have one to establish a Computer Security Incident Response Team (CSIRT). In September 2003, the U.S. and Bulgaria co-hosted a cyber security conference, intended to raise awareness and generate ideas for regional cooperation, attended by 16 East European nations.

To develop a common foundation for international critical infrastructure protection policies, the U.S. has sponsored and promoted the adoption of several UN General Assembly resolutions: Combating the criminal misuse of information technologies (55/63, 2001), Creation of a global culture of cyber security and the protection of critical information infrastructures (58/199, 2003), and Creation of a global culture of cyber security (57/239, 2003). These resolutions heighten international awareness to and provide us a common starting point for dealing with all nations on cyber security issues.

Again, U.S. private industry representation is key to many of these bi- and multilateral meetings as most critical infrastructures are owned and operated by the private sector. Industry participants articulate the need for security and protection of assets to foreign government and industries, share ideas and best practices for the development of CIP programs and in securing infrastructures, and frequently go on to develop long-term relationships with their foreign industry counterparts.

Assistant Secretary of State for Political-Military Affairs Lincoln P. Bloomfield, Jr.

The bottom line is that:

- It takes thoughtful and deliberate analysis to tie together the identification of critical infrastructures, with harmful vulnerabilities, and dangerous interdependencies between nations;

- Nations must work together to protect these critical services and assets, and thereby protect their populations and economies, as invisible borders do not serve to protect us from harm;

- Private industry is a vital partner in governments' efforts to protect their citizens and critical services, and;

- There is much work to be done by us all - nationally, regionally, and internationally - to improve CIP. ❖

24/7 Network

In a networked world, it is critical that public safety officials be able to contact officials in other countries on an emergency basis in order to identify the source of terrorist or criminal communications, investigate threats and prevent terrorism and crimes. Anyone can bypass national borders through new communications technologies and plan a crime in one part of the world from a physical location thousands of miles away.

In investigations involving computer networks, it is important for technically literate investigators to move very quickly to preserve data and locate suspects. Often, a criminal can only be stopped if evidence of his or her conduct is preserved within minutes or hours, a time-frame too short for reliance on traditional international assistance regimes.

Therefore, to enhance (but not replace) traditional methods of obtaining international assistance, the G8 created in 1997 a new mechanism to expedite contacts between countries in cases involving networked communications and other related technologies. The making of a request does not guarantee that the receiving country will assist - countries have many legitimate reasons to decline to assist each other - but it should ensure that the receiving country pays immediate attention to a request.

To date, 37 countries have joined a network of points of contact for cases involving electronic evidence. These contacts are available at all hours, 7 days a week, to receive information and requests for cooperation. The following countries have joined the 24/7 network:

Australia; Austria; Brazil; Canada; Croatia; Czech Republic; Denmark; Dominican Republic; Finland; France; Germany; Hong Kong, China; Hungary; India; Indonesia; Israel; Italy; Japan; Republic of Korea; Luxembourg; Malaysia; Mexico; Morocco; The Netherlands; New Zealand; Norway; Philippines; Romania; Russia; Singapore; South Africa; Spain; Sweden; Taiwan; Thailand; the United Kingdom; and the United States.

This network has been used successfully in many investigations in a number of countries. For example, the network has been used to help secure the conviction of a murderer in the United Kingdom by facilitating the preservation and disclosure of Internet records in the United States. The network has also been used on several occasions to avert hacking attacks, including attacks on banks in the United States, Germany and Mexico. ❖

Convention on Cybercrime

On November 23, 2001, in Budapest, Hungary, the United States and 29 other countries signed the Council of Europe Cybercrime Convention, the only multilateral instrument drafted to address the problems posed by the spread of criminal activity on computer networks. The Cybercrime Convention will require parties to establish laws against cybercrime, to ensure that their law enforcement officials have the necessary procedural authorities to investigate and prosecute cybercrime offenses effectively, and to provide international cooperation to other parties in the fight against computer-related crime.

The United States actively participated in the drafting of the Cybercrime Convention from the beginning. It also accepted comments and consulted repeatedly with representatives of the US technology and communications industry and a variety of public interest groups, especially after the draft text was first made public in April 2000. Ambassador Nancy Brinker signed the Convention on behalf of the United States. In order for the Convention to enter into force in the United States, it first must be ratified by the President, after the President receives the advice and consent of the Senate. On November 17, 2003, President Bush transmitted the Convention to the Senate with a view to receiving its advice and consent to (*Continued, Page 33*)

The Critical Infrastructure Economy

Valerie McNevin, Senior Financial Sector Specialist*
World Bank

Introduction: Birth of the Critical Infrastructure Economy

September 11, 2001 ushered in the millennium challenge: to build a safe and sound cyber commercial infrastructure. That day signified the transformation of the "Internet Economy" into the "Critical Infrastructure Economy", replacing the hype of the Information Age with the sobering realization that the Digital Age is fraught with weaknesses that we do not fully understand. One week later, on September 18th, we watched as Code Red, a malicious worm, spread across the globe, crippling businesses, disrupting services and disabling computers. Once again the world was reminded how susceptible to and dependent on technology it is. The wondrous promises of globalization, connectivity and interoperability were overshadowed by the reality that unplanned reliance on technology can result in disastrous and crippling results at the hands of a few. The bottom line was clear - to survive under the present business model, government and business must be proactive. Overnight the mandate became: Anticipate, Prevent and Mitigate the unacceptable levels of cyber and physical risk.

On the domestic front, Article 5 of the National Cyber-Security Strategy emerged from September 11, mandating the US to reach out and work with international institutions and multilateral agencies to create a "culture of security". By so doing, the US acknowledges that global interconnectedness requires us to think beyond assumed constraints, to recognize that cyberspace, by its very nature, cuts across borders-be they institutional, geographical, or jurisdictional. As such, multilateral organizations should be expected to play a significant role in developing critical infrastructures for emerging economies to engage in safe and sustainable development. In order to fortify efforts in the US, there is a need to take this mandate to the international stage and translate it into developmental reality.

Global Cooperation: The Role of Multilateral Organizations in the Development of Critical Infrastructures in Emerging Economies

Today over 200 countries are connected to the Internet and only a decade after its introduction into society, it has increasingly become the primary tool by which countries are reorganizing their economies. Across the world, countries, including emerging economies, are ever more dependent on technologies to support critical infrastructures and deliver essential services. This is especially true in every service area associated with finance, including payments and settlements.

UN Resolutions 57/239 and 58/199 , the OECD "Culture of Security" guidelines and the APEC Cyber-Security Strategy set out the beginnings of a framework for the sustainable development of critical infrastructure. Today, concept of critical infrastructure is quickly making its way through the vernacular, but more slowly at the economic policy level. It has not yet been translated into lending and technical assistance vehicles. As the euphoria of leapfrogging and economic surges give way to questions of financial stability and market distortion through unplanned or ill-planned growth, lending and technical assistance must align with the realities of this new age. Globalization efforts can no longer be solely for the purpose of opening markets and reaping quick profits but now requires serious thought and planning to achieve sustained development.

Developing countries wrestle with a number of issues, including underdeveloped industrial infrastructures, difficulties in growing money and in accessing investment/development money, transition to privatization, and different stages and levels of development. This means that their reliance on certain infrastructures most likely (*Continued, Page 25*)

**The views and opinions in this article are personal and do not reflect that of the World Bank.*

National Telecommunications and Information Administration Forging International CIP Ties

The National Telecommunications and Information Administration (NTIA) has represented the U.S. Department of Commerce in international critical infrastructure protection activities since 1998. In 1999, NTIA created the Critical Infrastructure Protection (CIP) International Affairs Outreach Committee comprised of government and industry representatives to provide practical perspectives on priorities for international CIP initiatives. The mission of the Committee has been to develop industry perspectives on international outreach for critical infrastructure protection, and to ensure, where appropriate, that industry is represented in the USG's international CIP discussions.

The stated objectives of the International Outreach Committee are to identify a good working relationship for industry and government in regard to CIP; identify industry's key international CIP issues; identify industry's priority countries for international CIP discussions; provide industry's views on key international issues and priority countries to the Department of State; to identify multilateral fora where CIP issues should continue to be discussed and new multilateral fora where CIP discussions should be introduced; suggest approaches for better coordination among international entities addressing CIP issues; and finally, to identify industry's interest in collaborative international research projects on CIP and ensure that viable proposals are coordinated with NTIA and the White House Office of Science and Technology Policy's R&D Working Groups on CIP.

In June, 2000, NTIA provided the Department of Commerce perspective to the Department of State on the Four Track Approach for International Outreach, which was the original CIP international strategy. Beginning in 2000, representatives from NTIA have participated in CIP bilateral discussions with Canada, Australia, the United Kingdom, Germany, India, Italy, and Japan.

As part of the U.S. Government interagency process, in 2002 a new bilateral approach was developed involving modular presentations for small U.S. delegations of 3-4 people to tailor the discussion to the interests and needs of particular countries. As part of the modular approach, NTIA created a Commerce Department presentation on CIP that includes promoting best practices, security standards, security technologies and services for economic growth (thereby ensuring a secure CIP framework for e-commerce to flourish), and public safety through use of spectrum efficient technologies.

NTIA has also led international discussions of security standards that were predicated on the success of the standards model that NTIA created for the U.S.-Australia CIP Bilateral (August, 2001). The standards discussed with the Australians included: Public Key Infrastructure (PKI) and Trust Models, Cryptographic Standards and Testing Programs, Internet Security Standards, Technical Security Standards: the Common Criteria, Network Security Standards, and Security Management Standards: ISO 17799. Additional topics for international discussion may include the need to develop standards for wireless priorities, interoperability, and enhanced 911 in order to coordinate emergency services. The need for such standards was made very clear at the time of the 9/11 attacks, which revealed the inability of emergency service providers to communicate with one another.

Multilaterally, NTIA has played an active policy role in the presentation of CIP issues in the Council of Europe (Cybercrime Convention), the OECD (revision of the Security Guidelines), APEC (introduction of the Common Criteria), the European Union (computer related crime treaty), and the G8. In 2002, NTIA hosted a trilateral standards meeting with the Australians and Canadians, which concluded with recommendations for follow-up (*Continued, Page 18*)

NTIA (*Cont. from Page 17*) discussions. More recently, NTIA participated in CIP multilateral programs in Buenos Aires (July 2003) and Sofia (September 2003).

Through bilateral and multilateral discussions, the U.S. Government has learned that achieving security and economic growth internationally involves dynamic interaction with other countries. Because the Internet and electronic commerce are inherently global in nature, critical infrastructure protection requires collaboration among international bodies and private sector enterprises in order to come up with worldwide solutions regarding security. With NTIA's leadership, the CIP dialogue with other countries has been strengthened by including industry representatives in the discussion. Industry participation in bilateral and multilateral discussions has shown that the private sector can play a key role in crafting the international CIP message - balancing national security and law enforcement goals with emphasis on economic security objectives.

From the beginning of international CIP activities, private sector companies identified several CIP priorities to be addressed in the international arena: Countering hacking, allowing strong encryption software, and protecting the privacy of Internet users. Electronic privacy and security controls must be developed more fully and deployed internationally. These are all issues in which NTIA plays a leading policy role. How these issues are handled internationally will determine the economic security of each country and the nature of the information society as a whole. ❖

International CIP Activities at DHS

Within the Information Assurance and Infrastructure Protection Directorate at the Department of Homeland Security, the Strategic Partnerships Office is helping to coordinate various international initiatives focused on critical infrastructure protection. Some examples of the efforts underway are:

◆ Establishment of formal working groups with Canada, and Mexico to focus on cross-border issues. There are numerous examples of shared critical infrastructures including pipelines, border crossings facilities, and electrical facilities, which need to be identified, assessed for vulnerabilities, and protected. This represents activity as a joint effort by the three nations.

◆ Establishment of formal agreements with multiple countries, including the United Kingdom, Australia, and Israel in order to provide for sharing best practices, methodologies, and processes about physical and cyber protection.

◆ Working closely with CERTS in other countries to establish relationships and regular communications in order to create an active network of CERTS around the world. The vision is to develop a global community to share cyber vulnerability and incident information as well as to work in concert in the event of a global incident. In addition, DHS is working with and encouraging those countries that have not matured their cyber security capabilities to develop this capacity.

◆ Sharing information with representatives from Sweden, France, Korea, Russia, Italy, Hungary, India, Germany, Japan and other countries to inform them of DHS initiatives in the CIP arena.

Cresencio (Cris) Arcos was appointed **Director of International Affairs for the U.S. Department of Homeland Security** in June 2003. The Office of International Affairs at DHS promotes information and education exchange with friendly nations, including: R&D on homeland security technologies; joint training exercises of first responders; and terrorism prevention, response, and crisis management. The office manages international activities within the Department. Prior to his role at DHS, Ambassador Arcos was the Vice President and Managing Director for International Public Affairs for Latin America and Canada with the AT&T Corporation (1995-2002). During this period, he also served as a Member of the President's Foreign Intelligence Advisory Board at the White House. Before working with AT&T, Ambassador Arcos retired with the rank of ambassador from the U.S. Department of State after a 25-year career. ❖

Towards a Global Critical Infrastructure?

Peter Mandaville, PhD
Center for Global Studies, George Mason University

Peter Mandaville

How can we incorporate a greater sense of 'globality'- that is, consciousness of the intense transnational interconnectedness that characterizes contemporary world society-into how we think about critical infrastructure? It is by now a truism to observe that the core structures of capitalist exchange, such as liberalized markets and the free flow of good and services, simultaneously give rise to our greatest vulnerabilities. Sociologist Ulrich Beck has described this condition as one of 'world risk society,' seeing in it an ever increasing "gulf between the world of quantifiable risk in which we think and act, and the world of non-quantifiable insecurities we are creating."[1]

So how can policymakers and security professionals best navigate the complexities of global risk when it comes to critical infrastructure? To be sure, some measure of unconventional thinking is called for - yet this would most appropriately take the form not of "thinking outside the box," but rather thinking through the box of sovereign territoriality; in short, a reimagination of the spaces and locations of critical infrastructure is called for. The tendency to date has been to think of critical infrastructure in terms of national security. This is understandable insofar as the primary concern of policymakers is always the safety and territorial integrity of the nation - to ensure, quite literally, the security of the homeland. In the wake of 9/11, for example, the tendency has been to batten down the hatches when it comes to critical infrastructure at home. But what if the hatches are somewhere else?

It can be reasonably suggested that in addition to the obvious components of national critical infrastructure-communications, energy, transportation, commerce, essential government, etc.-there exists today an emerging global critical infrastructure whose protection demands cooperation and legislation across various sectors in multiple countries and intergovernmental forums. Just as the Internet is itself composed of a collection of local networks, global critical infrastructure (GCI) can be conceived as a collectivity of national infrastructures.

Where is GCI? It is in the communications and data layers that permit the interconnection of national and regional air traffic control systems, such as the

(*Continued, Page 29*)

The Center for Global Studies (CGS) is a new central research unit dedicated to the promotion of multidisciplinary research on globalization. CGS coordinates outreach efforts in the area of global affairs, facilitating access for external communities to the University's full range of global expertise. CGS is comprised of more than sixty associate faculty members whose collective expertise spans the full range of the humanities, the social and natural sciences, information technology and engineering-as well as professional fields such as conflict resolution, public policy, law, management, and health. All CGS education, research and outreach is animated by a commitment to the cross-fertilization of knowledge and methods from multiple fields of study in order to better understand the complexities of globalization. The Center's work is structured around seven theme pillars: Globalization / Global Justice: Bridging the Divide; People Flows: Migration, Refugees, Diaspora; World Orders & Global Governance; Global Public Spheres: Media, Markets & Civil Society; Beyond West & Non-West: Dialogues on Culture & Ethics; Human Security, Conflict & War; Technology, Growth & Sustainability. CGS engages in a number of outreach and public education activities, including collaborative work with universities, think tanks, and other research centers and briefings and publications for policymakers and global affairs professionals in both the public and non-governmental sectors. CGS is a member of the Global Studies Network (GSN), an international consortium of university research centers dedicated to the study of globalization. Some of the Center's initial programs include: organizing an ongoing colloquium for faculty at DC-area universities with research interests in globalization; a research program studying the sociocultural impact of IT outsourcing in receiving countries; a guest speaker series around the theme of migration, refugees, and diaspora; coordinating a number of graduate certificates organized around various themes related to globalization, and a global cinema program for the DC-area communities.

U.S. - Canada Task Force Presents Final Report on Blackout of August 2003

August 14, 2003, saw the worst blackout in North American history. In early April, Spencer Abraham, U.S. Secretary of Energy, and the Honorable R. John Efford, Minister of Natural Resources Canada, released the Final Report of the U.S.-Canada Power System Outage Task Force. This report identifies the causes of the power outage and why the outage was not contained. It also presents comprehensive technical and policy recommendations to prevent or minimize the likelihood of future blackouts, and reduce the scope of those that do occur.

"I wish to thank the Task Force, and all those on both sides of the border, who contributed their hard work, skill and dedication. Their recommendations provide a roadmap for solving this critical international challenge." -- **Spencer Abraham, U.S. Secretary of Energy**

Recommendations include the following:

- Implementation of mandatory and enforceable electricity reliability standards in both the United States and Canada, with penalties for noncompliance, backed by appropriate government oversight;
- Strengthening the institutional framework of the North American Electric Reliability Council (NERC) and its initiatives on compliance;
- Developing a funding mechanism approved by regulators for NERC and the regional reliability councils, in order to ensure their independence from the parties they oversee;
- Addressing deficiencies identified in FirstEnergy and some reliability organizations in the United States, by June 30, 2004;
- Strengthening the technical recommendations made by NERC on February 10, 2004;
- Improving near-term and long-term training and certification requirements for operators, reliability coordinators and operator support staff; and
- Increasing the physical and cyber security of the network.

"The Final Report is a thorough examination of the electricity system before and during the blackout. It is very important that these recommendations be implemented. I am looking forward to working with Secretary Abraham, my provincial colleagues and industry in both Canada and the U.S. as we move to implement changes to reinforce the reliability of the North American electricity system." -- **John Efford, Minister of Natural Resources Canada**

After the publication of the Interim Report in November 2003, the investigation team probed further into the state of reactive power supplies in northern Ohio prior to August 14, 2003. The team found that the ability to supply reactive power within the area had been inadequate for several years, and that the regional reliability council had not previously identified this vulnerability. As a result, there are now four groups of causes of the blackout:

1. Inadequate system understanding;
2. Inadequate situational awareness;
3. Inadequate tree trimming; and
4. Inadequate reliability coordinator diagnostic support.

The Report also identifies seven violations of the voluntary reliability standards administered by NERC.

The Final Report is comprehensive and covers all work done through the three Working Groups: electric system, security and nuclear. The Working Groups drew substantially on the work of NERC and input from three public forums, two technical workshops and electronic submissions to the U.S. Department of Energy and Natural Resources Canada.

The Task Force reviewed previous major North American power outages and found that the causes of the August 14, 2003, blackout were strikingly similar to those of earlier outages. This finding reinforces the need for effective implementation of the Task Force (*Continued, Page 33*)

If It's Thursday, This Must Be Stockholm: The Critical Infrastructure Protection Project European Initiative

A characteristic feature of Critical Infrastructure Protection is its international nature, particularly in terms of managing the global digital infrastructure. The CIP Project Law & Economics Staff recently had the opportunity to strengthen the international focus on CIP by participating in two international conferences. The first was the UNCITRAL Commercial Fraud Colloquium in Vienna, Austria, and the second was the Comprehensive Risk Analysis and Management network (CRN) 6th Annual Experts Conference in Stockholm, Sweden. Between conferences, the Law & Economics Staff connected with the European Union Institute for Security Studies and the Secretariat General de la Defense Nationale.

UNCITRAL: Connecting CIP and Commercial Fraud

The CIP Project was a sponsor of the first United Nations Commission on International Trade Law (UNCITRAL) Colloquium on Commercial Fraud in Vienna, April 14-16, 2004. Participants included over 100 industry representatives, practitioners, regulators, and justice and trade officials who are engaged in the combat against international commercial fraud. The Colloquium was organized by the International Institute of Banking Law and Practice, whose director, Professor James Byrne, is also a professor at George Mason University School of Law.

In many areas, critical infrastructure protection and commercial fraud intersect. Most obviously, the cyber security aspects are quite similar. The methods used to break into computer systems and steal sensitive financial information are frequently the same used to attack computer systems for nefarious terrorist purposes. Thus, the same security practices that can save a system from terrorist attack can also save a system or company from commercial fraud. Familiar issues arise when financial or commercial fraud occurs: what is a corporation's responsibility to report when it has been defrauded? What is the duty of a corporation to disclose when its sensitive information has become compromised? These are the types of questions that the cyber security and critical infrastructure protection arenas have been grappling with for some time.

In addition to the computer and internet security concerns, commercial fraud encompasses money laundering - a tactic often employed by terrorists to surreptitiously fund their activities. Methods formerly used to trace organized crime activities are now being used to trace terrorists. However, as awareness of, and interest in, terrorist activities increases and more governments are taking steps to "follow the money," banks and other financial institutions are being pressed into service. Resources once used to serve customers are now used to perform internal investigations - a change that can affect a corporation's bottom line. And so, another familiar question arises: who pays? Should it be the government who initiates the investigation, or should it be the cost of doing business? Again, this is a question that the CIP has yet to decipher, and the commercial fraud world has just begun to tackle.

One area in which the CIP community can learn valuable lessons from commercial fraud is information sharing. As with CIP, information sharing is critical in stopping commercial fraud, particularly when new vulnerabilities or schemes are discovered. One particularly successful model is the North East Fraud Forum (NEFF), a regional group based in the UK. The NEFF brings together participants law enforcement, the government, and industry to share information and develop tactics for combating commercial fraud. This is accomplished primarily through training and conferences, which are free to NEFF members. Thus, the group is not only sharing information, it is also financially sustainable - a challenge for CIP groups in the US.

Paris: The EU Takes on "Homeland Security," and the French tackle Cyber Security

After the Commercial Fraud Colloquium, the Staff stopped briefly in Paris to meet with members of the French Government and the European Union. The

(Continued, Page 27)

Observations of An Innocent Abroad: Reflections on Security in a New Europe

by Anne Daily

The first time I went to Europe was ten years ago. As a woman of twenty, my only security considerations were of a personal nature: whether I had my passport and traveler's checks in my money belt; keeping my ticket and spare traveler's checks in the hotel safe; and doing my best to look like someone a mugger shouldn't mess with - in other words, scowling a lot.

On subsequent trips to Europe (all pre-9/11), I relaxed a little. I was a world traveler; I could make friends with the natives and practice my foreign language skills. Despite the fact that I was a woman traveling alone, I thought nothing of staying out late and walking around all parts of town. That is, until one night when a man followed me out of a bar and tried to get me into a car with him. I ran into the nearest hotel lobby and hid out until the coast was clear, and then I took a cab back to my own hotel. The experience was a little nerve-racking. I had trusted that I would be safe, and that trust was violated. I started to put the scowl back on my face.

Even before September 11th, my international traveling had been curtailed; I entered law school in the fall of 2000, and my trips to France and Italy were exchanged for trips to the law library. After September 11th, I saw how dramatically domestic air travel changed: random bag checks and body scans; removal of shoes to examine for bombs; and thousands of Swiss Army knives, once thought to be acceptable carry-on items for air travel, now left behind in every major airport (not to mention knitting needles and fingernail clippers.) You can't even get up to use the restroom within 30 minutes of departure or arrival at Reagan National Airport - no matter how much water you just drank. Gone are the days of the "three questions," asking you if you packed your own bags, if you'd left them unattended, or if you were carrying a package for someone else. Such old measures mirrored my relaxed attitude when traveling alone; the new measures were the equivalent of a scowl. This may not be a friendly system, but the world doesn't seem as friendly either.

Europe, it seems, has not yet put on this scowl - despite recent events such as the bombing in Madrid. The 25 countries that compose the European Union (10 of which just joined the EU on May 1st) embrace the "Elimination of Controls on Persons."[1] This means that when one enters a member country from another member country, most immigration, customs, and security controls are nonexistent. One can walk just as easily between Austria and the Czech Republic as one can walk between Virginia and Maryland. Controls are only at the external borders, so once you have entered the EU, you are as free to move about it as you would be to move about the United States - if not more so.

Anne Daily

After an almost five year hiatus, I finally made it to Europe this spring. I figured that European travel would be just as hectic as travel in the U.S. had become. When I arrived at my first destination, Vienna, I was surprised not to see long lines waiting to get through customs and immigration. I spent less than five minutes in line, if that. The woman checking us in barely looked at my passport. But I was even more surprised when I flew to Paris from Vienna a week later. In the Vienna airport, the only security check-point was at the gate. Imagine arriving at Dulles, taking the bus to your terminal, and walking all the way to your gate before walking through a magnetometer or putting your bags through the X-ray - pretty unlikely. When I arrived in Paris, I kept looking around for the immigration kiosk so I could show my passport, but to no avail. Once I was in the EU, nobody cared where I went.

The original and still primary goal of the EU is to create an economic bond between its member

(Continued, Page 28)

US - Canadian Security Relations

Conference Participant Perception
Catherine Lazarus

U.S.-Canadian Security Relations: Partnerships or Predicament?
April 15-16, 2004
Hilton Durham Hotel, Durham, NC

Sponsored by:
Center on Law, Ethics, and National Security (LENS), Duke University
Center for Canadian Studies, Duke University
Center for United States Studies, University of Quebec at Montreal
International Law Society, Duke University
Liu Institute for Global Issues, University of British Columbia
Terry Sanford Institute of Public Policy, Duke University
Triangle Institute for Security Studies (TISS)

Designated a Regional Meeting of the American Society of International Law

In April, Duke University and the University of Quebec at Montreal sponsored a conference entitled U.S. - Canadian Security Relations: Partnership or Predicament. The conference sessions, which covered a variety of topics such as border issues, counterterrorism, military cooperation and questions of law and NORAD/NORTHCOM, provided valuable insight into the complex issues surrounding the relationship of these two countries. The United States and Canada have historically been strong security partners, and their security requirements have often converged, as they share a large border, and the incentive to prevent foreign attacks through each other's territory.

Although Canadians are uncertain how they want to respond and cooperate with the United States' post September 11th policy shift to more proactive homeland security initiatives and new terrorist threat, they have continued to participate in two traditional security joint ventures, the Smart Border initiative and NORAD (North American Aerospace Command, a joint US-Canada venture to protect the airspace of Alaska, Canada and the contiguous 48 United States.). The continuation and expansion of these two successful ventures maintains positive relations between Canada and the United States and sets an example for future joint security efforts.

Imminent Threat

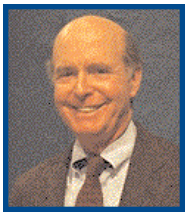
The attacks directly on U.S. soil and assets changed the mindset and policies of the current U.S. government. Many U.S. allies, including Canada, recognize there is an increased danger posed by a larger terrorist threat, but were not and have not yet been directly attacked. Canada and the United States recognize each country's security is dependent on the other, that one country's homeland security can be the other country's counterterrorism, and any defense against terrorism or security threat requires local, regional and national cooperation. Towards this goal, both the United States and Canada now use NORAD to survey for both external and internal threats. Canada continues to support several security joint ventures with the United States, including participating in NORAD and the Smart Border initiative described below. Having the United States alone on alert for a threat or warning is not as effective as having the U.S., Canada and Mexico working together.

The Border

One of Canada's shared borders with the United States is physical, and while each have seen success in jointly managing the border through traditional means, in December 2001, both countries also embarked upon a partnership called the Smart Border Initiative. This Initiative, which strengthens the border with a 30-point action plan to create the largest, longest unmanned border, was instrumental in creating bi-national steering committees on critical infrastructure protection and customs lookouts, as (*Continued, Page 31*)

International Center for Applied Studies in Information Technology

The International Center for Applied Studies in Information Technology (ICASIT) is a multi-million dollar international center on the GMU campus with IT projects in thirty countries on four continents. It sponsors studies on Information and Communications Technology (ICT) diffusion in the Muslim world as well as Africa, South America and Central Europe. ICASIT is a leading provider of up-to-date Knowledge Management information in the DC Metro region and sponsors the KM Round Tables at sites like NASA, SAIC, Mitre and the World Bank. The center is the focal point of a study sponsored by the Andrew W. Mellon Foundation which has developed convincing evidence that Distance Learning is much more expensive than previously thought.



Steve Ruth

ICASIT, located in GMU's School of Public Policy, is versatile, because its goal is to examine ICT diffusion, wherever it's happening. Professor Steve Ruth of the School of Public Policy, ICASIT's director, says that ICASIT's low profile is not surprising. "The kinds of reports we develop are sometimes counterintuitive —we often surprise our clients," says Ruth.

ICASIT has become increasingly interested in several Homeland Security issues, with particular emphasis on what Ruth calls the "quiet problems." For example, in his technology policy classes students have examined the relative danger and likelihood of various terror threats: nuclear, biological and cyberterrorism. "We use only the open literature, but it's interesting to see how much variation there is among experts about which of the types of terror threat are more feasible to implement", says Professor Ruth, who believes that currently a major cyberterrorism attack is less likely than other methods of terror delivery. Ruth's classes also study some of the less-publicized ICT public policy issues, like the importation of coltan, a vital mineral used in the manufacture of cell phones. "Most of the world's coltan comes from sources that are not exactly leaders in democracy-so we ask ourselves whether governments should take a stand on this," says the professor.

The major funding for ICASIT's activities has been in implementing ICT solutions in over thirty poor nations, primarily in Africa and Asia. The typical project involves helping to set up a linkage between an overseas university study center and a U.S. institution. One of Ruth's projects linked the School of Public Health at Uganda's Makerere University in Kampala with the counterpart institutions at Johns Hopkins and University of North Carolina. As part of this work ICASIT has developed a large world database of ICT indicators, with particular emphasis on Muslim and Arab nations. Ruth, who taught a course last year called "Islam and the Internet" has become interested in ICT deployment among the nearly 60 predominantly Muslim nations. He feels that there may be some links between high levels of ICT development and lower incidence of terrorism. But the link is sometimes tenuous. "If you look at the numbers for the United Arab Emirates, they are similar to those of France and Germany. On the other hand, that's also true of Israel."

Ruth is hopeful that the three ICASIT research specialties--international ICT diffusion, validation of distance learning costs and leveraging of Knowledge Management-can be linked to the Homeland Security agenda. "I think we have a lot to offer in that arena—our approach is seasoned by our extensive international experience on other projects," says the professor. ❖

SeongKyung Cho is a CIP Project International Fellow working on a post-doctoral fellowship at GMU's Tech Center. Her research is on citizen participation in U.S. energy policy. Ms. Cho is a native of Seoul, Korea and is a researcher at the Korean Society for Risk Governance.

Economy (*Cont. from Page 16*) will be different than that of the developed world. Emerging economies differ from developed countries in another very real aspect. Most of the critical infrastructure in these countries is not privately owned. Since the government owns it, it is in some ways easier to require that it meet certain standards. But finding the money as well as the technical capacity to protect it are over-riding factors. The US should use this reality in a way that benefits all parties, since in a networked economy, the health of critical infrastructures in other countries ultimately affects that of our own.

Efforts of the World Bank Financial Sector

Three years ago, the National Strategy to Secure Cyberspace tasked the US Financial Sector to create its own roadmap to secure an industry that has become intensely dependent on information infrastructure. It has yet to be accomplished. The World Bank Financial Sector is examining a slice of the cyber-critical infrastructure quagmire by examining the double-edged sword nature of financial access via open network architecture. For developing countries expanded access to financial services through new information infrastructure technologies promises significant opportunities for growth and development. However, studies confirm that increased access through technology is always accompanied by attendant increases in cyber crime, penetrations and disruption that result in corruption, destruction of data and/or denials of service. The result is downward pressure on efficiencies and productivity gains coupled with an increased threat to the operational integrity of key critical infrastructure systems and personal privacy of information in the system.

In the book published by the World Bank entitled "Electronic Safety and Soundness: Securing Finance in a New Age" my colleagues and I set forth a framework composed of four pillars which are crucial to and should be developed in parallel with the financial services information infrastructure. These are the legal and regulatory framework, human resource training and education, public-private cooperation, and layered security. These four pillars are essential to the sustainable development of any critical infrastructure, in any country undergoing any stage of development.

On September 17 & 18, 2004 in Singapore, the World Bank with the cooperation of the Association of Banks in Singapore and the Monetary Authority of Singapore jointly sponsored a conference entitled "Asia Pacific Regional Conference on Electronic Safety and Soundness." This marked a significant step forward in responding to the need for increased understanding and awareness of issues related to critical information infrastructure in the financial sector. Over 17 countries from the APEC region attended with representatives from central banks, financial regulatory authorities, private companies and academic institutions to discuss cross-border cooperation, the rise of cyber-crime, the particular vulnerability of the financial sector's stability in this environment and the operational risks imposed on all countries by an openly connected global economy. The double edged nature of the e-financial revolution was discussed, with particular focus on the deficiencies in cross-border cooperation, layered security and supervision. The conference substantiates that people worldwide are keenly aware that technology is a powerful force, driving sea changes within our organizational, regulatory and economic structures and actively seeking answers to the paradoxical questions its use poses.

International Framework for Cooperation

While all countries are moving to greater reliance on open network architecture, critical infrastructure analysis will yield different results in emerging economies depending on the state of development of the markets and infrastructure build out. Although both developed and developing countries share certain common critical infrastructure, such as energy, power and connecting points to communicate and act on information, emerging economies are using it as core infrastructure while developed countries are migrating to this model for their core structure. Seemingly overnight, this information infrastructure has become essential to (*Continued, Page 26*)

Economy (*Cont. from Page 25*) economic survival and sustainable development.

Legal and other systems feel the pressure to provide answers to the paradoxical questions being posed as the need for information to protect national security and provide competitive trade advantages wars with individual privacy and consumer protection concerns.

The UN Resolution, OECD, and APEC are all serious responses to the call for collective will to create a sustainable critical infrastructure economy. The first imperative of such an economy is to build on and learn from the information that exists. To date, all information points toward the need to better understand, identify, and protect our critical infrastructure. Avenues are available through which we can continue to push forward the agenda of sustainable critical infrastructure development. The Millennium Challenge Corporation is one such vehicle, the World Bank is another. Together with cooperation from these entities through lending and aid criteria, emerging economies can grow in a safe and sound manner.

Critical infrastructure protection is fundamentally important to sustainable development. Going forward it is important that the World Bank and other multilateral entities substantiate the importance of cyber security and protected critical infrastructure through vehicles such as adjustment lending and technical assistance loans to emerging countries. Without this, the digital divide will grow ever larger and the unfulfilled promises made by technology may result in increased unrest and escalating violence. This is compounded by the reality that the potential to experience serious worldwide effects increases as we increase our dependency on the open network architecture, and on each other.

Thus, the development of the critical infrastructure economy may be at odds with the mantra of globalization; "access, availability and interoperability". September 11 showed us that in a globally connected world, whether we like it or not, risk knows no borders and is no respecter of countries. Failures in one sector bleeds over to other sectors - as well as worldwide-and can cause ripple, network, and/or cascading effects. Given this new reality, access must now be seriously debated and scrutinized.

Today, development needs to align with the lessons learned since 2001. Countries should move towards planned development and international lending efforts should apply critical infrastructure analysis so as to thwart over-reliance and critical dependencies on technology. The world over, countries are just beginning to grapple with how to define their critical infrastructures in the face of an over-dependence on open network technologies for globally interconnectivity. Much of the difficulty lies within the scope of three fundamental questions: What is a critical infrastructure, what does it do and how? In short, addressing these fundamental issues requires a critical analysis on both the domestic and international sphere. In turn, the results of this analysis should drive the creation of policy and the nature of aid and lending into the foreseeable future.

The World Bank Financial Sector strives to be an objective clearinghouse for information related to electronic safety and soundness to the sustainable development of financially related critical infrastructure. Please visit us at www.worldbank.org/finance. ❖

CIPP Europe (*Cont. from Page 21*)
European Union Institute for Security Studies, a think-tank that advises the EU Council, has its headquarters in Paris. The Institute deals with homeland security-type issues on both the EU and national levels. Of particular interest were the developments in the EU after the Madrid bombing. The event pushed countries to enact laws and develop strategies similar to those adopted in the United States after September 11th. This included international arrest warrant agreements, developing a common definition of terrorism, sharing flight passenger data with the United States, and creation of an EU terrorism czar.

This is not to say that the EU members were not active in anti-terrorism activities before the Madrid bombing, but they were perhaps less vocal about it. One stark contrast in strategy between the EU and the US is in the use of training exercises for emergency preparedness. In the U.S., these are performed with relative frequency, at local, state, and federal levels, and are extremely well publicized. Each exercise represents an opportunity to fine-tune and improve the system (as well as demonstrate how well the system is doing). In the EU countries, these exercises are low-key: often performed at night, with little or no publicity, and less emphasis on "lessons learned." Additionally, there is no standardization for preparedness - each country has its own system, its own training methods, and its own views of CIP - facts that complicate most EU-wide security initiatives.

While in Paris, the CIP Project Staff also took the opportunity to meet with members of the French Government who deal with cyber security issues. This falls primarily within the Secretariat General de la Defense Nationale (SGDN), Central Directorate for Information Systems Security (DCSSI). They provide the scientific and technical backbone of the French cyber security architecture, and provide counsel to the other ministries on technical issues. Their missions include high-level regulatory functions, as well as operational-level training and education.

The DCSSI works to strengthen information security within the government. Unlike the U.S. cyber security efforts, which focus primarily on the private sector, the DCSSI is an internal government operation. In part, this is due to the fact that many of the traditional critical infrastructures in France are either owned by the government directly, or are very closely tied to the government. As a result, external regulation is not necessary.

The visits to the EU and the French government provided a compelling snapshot of CIP and CIP-related work in Europe. They highlighted the many differences between the U.S. and Europe, which need to be understood in order to further any international CIP agenda.

If it's Thursday, this must be Stockholm: Civil Defense in the New Age

The final stop during this busy week was Stockholm, for the Comprehensive Risk Analysis and Management Network (CRN)'s 6th Annual Experts Workshop. This year's topic was Societal Security and Crisis Management in the 21st Century, with an intimate group of forty participants representing eight countries. The CIP Project was asked to discuss its work in the National Capital Region - Critical Infrastructure Vulnerability Assessment Project, as well as compare and contrast the notions of federalism in the US versus the EU. It was an honor to be included among such a broad and experienced group of security experts.

Although the meeting was only two days long, the participants were able to explore a variety of security issues. The presentations were broken up into two panels, with each panel followed by a detailed group discussion, or workshop. The first panel discussed the challenge of security threats and emergencies in modern society. This included presentations on the new Swedish Security Strategy, which focuses on a coordinated effort between state and local entities; on whether or not "comprehensive security" was achievable; and on how to approach risk and uncertainty in creating a security management strategy. After the presentations, the participants were broken up into two groups, and (*Continued, Page 28*)

CIPP Europe (*Cont. from Page 27*) were charged with discussing and answering the following questions:

- What is the specific content of emerging security panorama in regard to the nation-state's responsibility?
- What challenges do the management of threats and vulnerabilities in modern society create?
- What are the objectives and rationale behind the concepts? How applicable are they?

Each discussion group found difficulty in answering these questions, for they elicited even more questions. How much of the security panorama is the nation's responsibility, and how much belongs to the private sector? What do we mean by threat? By vulnerability? The discussions were lively and informative, and demonstrated that while each country may have different assets to protect, they are all having difficulty in finding the most effective way of protecting them.

The second panel discussed the distribution of responsibilities and funding when dealing with societal security, public safety, and emergency management. The kick-off speech was a scholarly presentation that evaluated the various regulatory mechanisms. The presenters, Dr. Jan Joel Andersson and Andreas Malm, discussed the differences between direct regulation (which is favorable to government, but not to industry), economic regulation, using incentives (which is favorable to industry, but hard for government to gage accountability), and public-private partnerships (which ideally optimize the relationship between government and industry.) Importantly, these are the questions that the CIP Project also focuses on when it engages new projects. As in the U.S., it was difficult for the international group to come up with a concrete definition of what a public-private partnership should be, or how it should work. This presentation concluded a compelling and productive first day.

The second panel resumed on the second day with presentations on: risk finance; the shift of responsibilities between government and society; risk-based defense planning; and the CIP Project's presentations on the NCR Project and federalism. After these presentations, the group was again divided and asked to answer certain questions. These included:

- How can vertical and horizontal security and safety cooperation be optimized?
- Who should set preventive priorities and define security standards?
- Who pays for, and would benefit from, dealing with vulnerabilities?

The last question - essentially asking who pays for security - garnered the most discussion during the workshop. As many pointed out, ultimately we will all have to pay - whether through our tax dollars (if through the government) or increased prices for goods and services (if through industry.) However, which of these mechanisms is the most effective and efficient is still unknown - and perhaps will be for quite some time.

This opportunity to engage and work with security and financial experts from all around the globe was tremendous. It represents an important step toward bringing the CIP Project's mission - combining law, policy, and technology to strengthen critical infrastructures - to a global level. ❖

Innocent Abroad (*Cont. from Page 22*) countries, with each country retaining its sovereignty and individuality. By eliminating border controls, trade and tourism flow more freely between the countries, increasing everyone's economic potential. However, this openness could have a potentially dangerous side effect in increasing the risk of terrorism. Each member country is reliant on the others to maintain effective security controls against those who are entering the EU from a non-EU country. France must trust that Slovenia (or Latvia, Poland, Spain, or Italy - or any one of the other member countries) is checking passports effectively and controlling access to the EU. So EU security has become a least common denominator calculus. One hopes that it is not just a matter of time before this trust is abused, and another attack like Madrid - or 9/11 - happens again on either side of the Atlantic. ❖

Globalization (*Cont. from Page 19*) European Union's EUROCONTROL project. We see it also in the financial clearing houses that permit portfolio flows to converse across polyglot national currencies. The non-sovereign spaces of the ocean and atmosphere are increasingly crucial for both commerce and security-both of which by their very natures resist an exclusively national approach to critical infrastructure protection. Without a doubt, borders and ports still matter, however they are only our most proximate entry point. In the absence of sufficient cybersecurity measures, the borders of America's critical information systems are just as much in China or Russia as in New York or San Francisco. Their critical infrastructure, in other words, is our critical infrastructure. And we better make certain that we are on the same page as our partners and allies in terms of how we understand the boundaries and nature of critical infrastructure. Regional integration is gathering momentum in various parts of the world, with the EU as the most advanced model in legal, economic, and political terms. But this process is also at our doorstep. As NAFTA deepens its structural tendrils, American, Canadian, and Mexican infrastructures become increasingly interdependent. With the recent advent of CAFTA and the quickening march to FTAA, critical infrastructure becomes a hemispheric concern. As globalization "thickens," to use Joseph Nye's terminology,[2] more and more of what we value and seek to protect on the home front will be connected to and dependent on larger scale processes of communication and exchange. The protection of critical infrastructure is an inherently global mission.

[1] Ulrich Beck, 'The Terrorist Threat: World Risk Society Revisited,' Theory, Culture & Society, Vol. 19, No. 4, 2002, p. 40

[2] Joseph S. Nye & John Donahue (eds.), Governance in a Globalizing World, Washington D.C.: Brookings Institution Press, 2000.

Peter Mandaville is Director of the Center for Global Studies at George Mason University and a faculty member in the Department of Public & International Affairs. ❖

Societal Security (*Cont. from Page 9*) across society as a whole. However, the benefit of regulation must be weighed against its potential costs. Given the problems of imperfect information, distributional consequences, and international markets, it is unlikely that governments will choose regulation as their first choice in ensuring appropriate emergency preparedness across society as a whole. Private firms, in turn, will most likely consider regulation to be the least desirable form of market intervention to correct the undersupply of emergency preparedness.

Jan Joel Andersson

Economic Policy Instruments

Rather than forcing the private sector by law, the government may use economic policy instruments - such as direct government subsidies or tax incentives - to encourage the private sector to invest in emergency preparedness measures voluntarily. It is likely that different types of incentives will be the first choice for private actors since it would allow them to improve their emergency preparedness measures on their own terms while avoiding both costs and government control. However, in using economic policy instruments, the government faces a trade-off between inducing the firms to behave in the desired way and offering them some socially costly rewards, rents. In fact, economic policy instruments will likely be the least appealing alternative for governments.

Andreas Malm

Public-Private Partnership

Given the problems of ensuring

(*Continued, Page 30*)

Societal Security (*Cont. from Page 29*) adequate levels of emergency preparedness in society by direct regulation or economic policy instruments, Public-Private Partnerships provide a solution that seems to satisfy both government and private actors. For the government, PPP provides a mean to engage the private sector in public affairs and to achieve guidelines and standards without having to resort to regulatory means of "command and control." Public-Private Partnerships are also preferred to direct subsidies or tax incentives since certain control can be maintained. For private actors, Public-Private Partnerships offer a flexible way in which to meet government requirements while avoiding regulation.

However, despite the general consensus on the positive aspects of Public-Private Partnerships, we argue that it may be an unreliable and unpredictable solution to the problem of closing the gap in national emergency preparedness and crisis management in deregulated sectors of the economy. There are several reasons for this argument. It is difficult to achieve tangible results with PPP. The main problem lies in implementation. It is relatively easy for government and private actors in a PPP to agree on the existence of a problem and that something must be done about it. It is, however, much harder to agree on what should be done about it, who should be responsible for implementing it, who should assume legal responsibility for it, and the who should bear the costs for the implementing it.

By refraining from imposing regulation and engaging in Public-Private Partnerships, the government pushes the responsibility for implementation and costs on to industry. Industry, in turn, will be reluctant to accept the responsibility and costs without clear guidance and economic compensation. Without clear guidance and money from the government, there is a distinct possibility that private actors simply participate in PPP as a means to deflect attention from insufficient emergency preparedness measures and to avert outright regulation. The preference ordering of the Government and the private sector of alternatives for closing the gap is illustrated in the figure below where 1 indicates the most favored solution, 2 the second choice solution, and 3 the least favored solution.

Figure Two: Closing the Gap

		Alternatives		
		Direct Regulation	Economic Policy Instruments	Public-Private Partnership
Actors	Government	2	3	1
	Private Sector	3	1	2

Source: Adapted from Jan Joel Andersson, "Public-Private Partnerships and Emergency Preparedness," paper presented at the conference on National Deregulation and European Reregulation, organized by the Stockholm Centre for Organisational Research, Stockholm, 27 February 2004, p. 8.

Conclusion

Despite the general consensus on the positive aspects of PPPs, we have argued in this paper that such partnerships may be an unreliable and unpredictable solution to the problem of closing the gap when it comes to issues of national emergency preparedness and crisis management in deregulated sectors of the economy. Our conclusion is based on theoretical as well as our own empirical work. Most importantly, it is difficult to achieve tangible results with PPPs. The main problem lies in implementation. In order to successfully close the gap in the provision of emergency preparedness measures, clear guidelines and recommendations, consensus among actors, time, and money are necessary. In other words, governments and private actors must reconcile responsibilities and costs in the provision of societal security.

[1]For a similar conclusion, see Peter Orszag, Testimony before the National Commission of Terrorist Attacks Upon the United States, November 19, 2003.
[2]For a more complete discussion, see Jan Joel Andersson and Andreas Malm. "Minding the Gap: Reconciling responsibilities and costs in the provision of Societal Security", paper presented at the conference on Societal Security and Crisis Management in the 21st Century - 6th International Expert Workshop, Stockholm, April 23, 2004. Available at http://www.isn.ethz.ch/crn/_docs/Andersson_Malm.pdf

For correspondence: andersson@ui.se; andreas.malm@4cstrategies.com

CIP Project Announces Third "Critical Conversation" June 29 Event to Address Port Security

As the July 1, 2004 deadline quickly approaches for the successful implementation of the Maritime Transportation Security Act (MTSA) and the International Maritime Organization (IMO) International Ship and Port Facilities Security Code (ISPS), the CIP Project will convene a debate between government and industry on the security of our ports as part of the international supply chain. Third in a series of "Critical Conversations" hosted by the CIP Project, the event will address issues concerning preparedness for the July 1 deadline, fiscal limitations, and the balancing act between the free flow of commerce against ever-tightening security and privacy concerns. The Conversation will seek to explore the Act's effectiveness as a policy matter and the feasibility of implementation.

This event will be held on June 29th at the National Press Club.

Since January 2004 Willem Holleman has been working with the CIP Project as an International Fellow. He is on sabbatical from his native Netherlands until the end of October. In the Netherlands, Mr. Holleman is a division manager and policy advisor for freight transportation at the Ministry of Transport. At the CIP Project, he is doing research on port security. His work will result in a critical conversation on port security by Frank Sesno at the Press Club in Washington on June 29. The critical conversation will focus on the policy challenges after the Maritime Transportation Security Act is fully implemented by July 1.

US-Canada (*Cont. from Page 23*) well as information sharing for visas criminal records. Both countries are jointly investigating different risk management initiatives to incorporate into the Smart Border Initiative to identify known travelers and known goods through identification procedures. These programs will allow frequent travelers faster border passage, while identifying unknown travelers and threats more quickly and easily. These initiatives include fast lane access with traveler card identification, container security initiatives, cross-border crime prevention and Integrated Border Enforcement Teams (IBET).

Missile Defense

Another timely conference component focused on the upcoming August activation date of the missile defense system. While Canada is in the process of determining their inclusion within this system, an echoing theme of this discussion centered around the "intervulnerability" of the U.S. and Canada. Geography, combined with the unknown asymmetrical threats terrorists pose, opens Canada to the possibility of a weapon or attack aimed at the United States hitting Canada, whether intentional or unintentional. To further increase the complexity of this "intervulnerability", Canada and the U.S. do not share just one physical border that must be protected, but all borders, air, sea and land must now be secured against both internal and external threats.

Conclusion

This two-day conference highlighted the complexities of the ongoing effort to secure and protect both the U.S. and Canada, and the united efforts that span the two nations. While there are a variety of variables yet to be defined and challenges yet to be faced as these countries move forward, the partnership provides a strong foundation to deal with these issues surrounding trade, border security and military defense. ❖

Canada (*Cont. from Page 5*) legal tools to enhance their applicability to emergency response and recovery.

Major emergencies require extremely close co-operation between the federal government, provinces and territories, communities, first line responders and the private sector. National emergency coordination currently suffers from the absence of both an effective federal-provincial-territorial governance regime, and from the absence of commonly agreed standards and priorities for the national emergency management system.

The Government will therefore invite provinces and territories to establish a permanent, high-level forum on emergencies in order to allow for regular strategic discussion of emergency management issues among key national players. The Government is also committed to moving ahead on the co-location of federal, provincial and territorial emergency operations centers. To this end, it will work with its provincial and territorial partners to put this in place where practical.

The Government needs to be able to continue to provide core services to Canadians during emergencies. Building on existing work in this regard, federal departments will ensure that they can continue to serve Canadians regardless of circumstances by strengthening their continuity planning processes and requiring regular exercises to test these plans.

Critical Infrastructure and Cyber-security

Critical infrastructure protection is one of the main challenges of modern emergency management. Most of Canada's critical infrastructure is owned by the private sector or other levels of government, and much of it is connected to international networks.

To establish a basis for the federal, provincial and territorial governments and the private sector to meet the critical infrastructure protection challenge, the Government will release a position paper setting out the key elements of the proposed Critical Infrastructure Protection Strategy for Canada this summer. The Government will consult senior-level provincial, territorial and private sector leaders to inform this strategy. Key international partners such as the United States will be part of this consultation process. The Government will work with provinces, territories and the private sector to drive forward a national process that prioritizes substantial improvement of national capabilities in critical infrastructure protection.

Cyber-security is at the forefront of the transborder challenge to Canada's critical infrastructure. The threat of cyber-attacks is real, and the consequences of such attacks can be severe. To achieve a more proactive cyber-security posture and to keep pace with the efforts of key allies, the Government will strengthen its capacity to predict and prevent cyber-attacks. To this end, the Government will substantially improve threat and vulnerability analyses for its systems, and strengthen its ability to defend its systems and respond to cyber-incidents.

The Government will also convene a high-level national task force, with public and private representation, to develop the National Cyber-security Strategy to reduce Canada's vulnerability to cyber-attacks and cyber-accidents.

Bringing Key Players to the Table

The federal Government is often not a lead player in emergency management. Consequently, the Government will initiate a process with its partners in the provinces and territories to bring key emergency management actors from across the country to the table. This includes communities, first line responders and the private sector. The objective will be to collectively assess the requirements of the entire national emergency management community to better position the country to meet the increasingly complex security environment that Canada faces.

The Government will work with provinces and territories at key meetings of federal, provincial and territorial security ministers and deputy ministers this summer. The Government will propose four strategic areas as national priorities:

- building operational capacity and seamlessness across the

(*Continued, Page 33*)

Canada (*Cont. from Page 32*)
national system, including strengthening surge capabilities;

- developing a broad process that includes the private sector and will lead to the Critical Infrastructure Protection Strategy for Canada;
- staging regular national and international exercises involving civilian and military resources to assess the adequacy of the national system against various emergency scenarios; and
- working closely with allies, particularly the United States, to continuously improve capacity and coherence in continent-wide emergency management.

Securing an Open Society: Canada's National Security Policy can be read in full at www.psepc.gc.ca/national_security/publications_e.asp ❖

CIP Oral History Project

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

Please visit the CIP Oral History website at http://echo.gmu.edu/CIPP/ where you will find a description of the project, members of the research team and a survey that asks about your views and your own role in critical infrastructure protection.

Cybercrime Convention (*Cont. from Page 15*) ratification. Should the US ratify the Convention, no changes to US law would be required.

The Convention breaks new ground by being the first multilateral agreement drafted specifically to address the problems posed by the international nature of computer crime. Although the obligations and powers that the Convention requires countries to undertake are already provided for under United States law, the Convention makes progress in this area by (1) requiring signatory countries to establish certain substantive offenses in the area of computer crime, (2) requiring Parties to adopt domestic procedural laws to investigate computer crimes, and (3) providing a solid basis for international law enforcement cooperation in combating crime committed through computer systems. ❖

Blackout (*Cont. from Page 20*) recommendations. We expect the collaboration between our two countries to continue as we implement the recommendations of this report. As a result, the Task Force mandate has been extended by one year, underscoring the two governments' commitment to ensuring that the recommendations are acted upon. This collaboration will also facilitate the necessary ongoing work by a number of federal, state and provincial government departments and agencies, and industry reliability organizations, as well as the industry itself on both sides of the border.

Canada's Prime Minister and the President of the United States established the Canada-U.S. Power System Outage Task Force on August 15, 2003, to identify the causes of the blackout that affected North America, and to make recommendations toward reducing the likelihood of future outages.

The report is available at https://reports.energy.gov and http://www.NRCan.gc.ca ❖

US Coast Guard International Activity

Captain Anthony Regalbuto (retired) is the Chief of Policy and Planning for the Coast Guard's Port Security Directorate. Within this position, he is involved with the International Port Security Program, which helps the United States and its maritime trading partners better protect the global shipping industry by facilitating the implementation of security improvements at port facilities around the world.

The Coast Guard conducted its first visit to Singapore several weeks ago to prototype its program. The next visit will commence next week in Honduras. The Coast Guard plans to visit 45 countries a year and 135 countries in a three-year cycle, since about 130 countries trade with the U.S.

As part of this effort, the Coast Guard and the host nations will work jointly to evaluate the countries' overall compliance with the International Ship and Port Facility Security Code, an international agreement signed in December 2002 that will enter into full force on July 1, 2004. In addition, the Coast Guard will provide assistance with interpretation of the international code, as it has already done through discussions with representatives from over 50 nations. The Coast Guard is working very closely with Customs and Border Protection to ensure that this program, the Container Security Initiative and other programs are developed and executed in harmony. ❖

"Second perhaps only to the global information network, maritime security is the most integrated infrastructure internationally. The U.S. Coast Guard is pleased to work closely with the international maritime community to secure our collective interests." **Captain Anthony Regalbuto (Ret.), Chief of Policy and Planning, U.S. Coast Guard Port Security Directorate**

The **5th Annual SecurE-Biz CxO Summit and Leadership Awards** will be held June 10 - 11 at the Marriott Metro Center in Washington, DC. The annual summit was established in 1999 by the Office of Secretary of Defense to provide an interactive, educational program where the world's leading practitioners share best practices and lessons learned in conducting secure e-Business. The theme for the Spring 2004 SecurE-Biz CxO Summit is: "Roadmaps for Enabling Secure Information Infrastructure and Cyber-Defense". CIP Project Director John McCarthy will be speaking, along with 70 other CxOs. For more information go to www.secure-biz.net.

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.