THE CIP REPORT

CRITICAL INFRASTRUCTURE PROTECTION PROGRAM VOLUME 5 NUMBER 12

JUNE 2007

INTERNATIONAL CIP

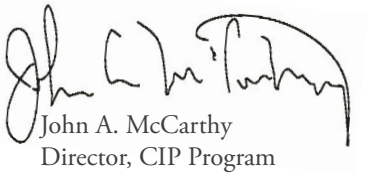
GEORGE MASON UNIVERSITY
School of Law
CRITICAL INFRASTRUCTURE PROTECTION PROGRAM

This month's issue of *The CIP Report* provides a yearly update to our International edition, highlighting the work done around the world by various international organizations and countries relating to critical infrastructure preparedness.

While the selections included provide only a glimpse into the diverse array of initiatives underway, they serve to highlight the details and nature of critical infrastructure protection as it is practiced around the world. We are pleased to include contributions from Canada's Office of Public Safety and the United Kingdom's Centre for the Protection of National Infrastructure (CPNI). In addition to their articles, we also feature a collection of newly compiled international definitions of critical infrastructure, which has resulted in the development of two interactive maps. The included article offers a brief summary and comparison of the international definitions of critical infrastructure representing 11 countries, three international organizations, and one project funded by the European Commission. We have also included an overview of international government and organizationally issued reports concerning critical infrastructure protection and national security for various countries and regions. We have also provided an overview of the European Network and Information Security Agency (ENISA) and their comments on the recent cyber attack on Estonia, as well as a directory and links to European Union Computer Emergency Response Teams (CERTs).

Our Legal Insights column is focused on Quarantine and Isolation, an issue that recently received international attention in May over the travel of a TB patient and the subsequent order of isolation issued by the Center for Disease Control. Finally, we include a brief article on a symposium organized by the CIP Program, Syracuse University's E-Governance Program and the Swiss Ecole Polytechnique Fédérale de Lausanne on the technical, legal, and political options for securing root zones, and an article showcasing recent additions to the CIP Program's digital library.

As always, we appreciate your continued support of the CIP Program and welcome your comments and contributions.



John A. McCarthy
Director, CIP Program
George Mason University, School of Law

Protecting the United Kingdom's Critical National Infrastructure (CNI)

CPNI
Centre for the Protection of National Infrastructure

The UK, like the US, is under threat from international terrorists. Al Qaeda and their associates and followers around the world understand the value of causing economic damage and have shown intent to attack CNI targets in sectors like energy, transport and finance.

Protection of the CNI is an important part of the PROTECT strand of the UK's counter terrorism strategy, CONTEST (see www.mi5.gov.uk; or www.homeoffice.gov.uk for further details of the strategy). Other parts of the PROTECT strand deal with the protection of crowded places, e.g. stadia and iconic sites, and of hazardous materials and dangerous substances.

CPNI is the lead provider of protective security advice to the UK's CNI. Formed on 1 February 2007 from an amalgamation of different organisations which led on physical, personnel and electronic protective security, CPNI aims to provide holistic, integrated protective security advice to the UK's CNI (further details of CPNI can be found at its website - www.cpni.gov.uk). It is a multi agency body comprising security specialists, government civil servants, and private sector employees.

CPNI works closely with the Government departments responsible for the nine CNI sectors (energy, water, food, transport, finance, emergency services, communications, health and government) and with private sector operators and owners. It seeks to mitigate the risk of attack by reducing the vulnerability of key sites, processes and systems. CPNI's approach is *impact driven, vulnerability focused, threat informed.* Protective security in the UK is delivered largely in an unregulated environment. Trust and transparency are fundamental to the relationship between CPNI's security specialists and the private sector.

Our advice aims to reduce the vulnerability of the national infrastructure to terrorism and other threats, keeping the UK's essential services safer.

The UK has significant experience of the need to protect infrastructure from terrorism, and has well-established protective security regimes in sectors like energy and water. But the latest manifestation of the *(Continued on Page 13)*

CPNI's Top ten security guidelines

Whether you are creating, reviewing, or updating your security plans, keep these key points in mind:

- Carry out a risk assessment to decide on the threats you might be facing and their likelihood. Identify your vulnerabilities and the potential impact of exploitation.
- If acquiring or extending premises, consider security at the planning stage. It will be cheaper and more effective than adding measures later.
- Make security awareness part of your organisation's culture and ensure security is represented at a senior level.
- Ensure good basic housekeeping throughout your premises. Keep public areas tidy and well-lit, remove unnecessary furniture and keep garden areas clear.
- Keep access points to a minimum and issue staff and visitors with passes. Where possible, do not allow unauthorised vehicles close to your building.
- Install appropriate physical measures such as locks, alarms, CCTV surveillance, complementary lighting and glazing protection.
- Examine your mail-handling procedures, consider establishing a mailroom away from your main premises.
- When recruiting staff or hiring contractors, check identities and follow up references.
- Consider how best to protect your information and take proper IT security precautions. Examine your methods for disposing of confidential waste.
- Plan and test your business continuity plans, ensuring that you can continue to function without access to your main premises and IT systems.

Canada's Approach to Critical Infrastructure Protection

Critical infrastructure protection plays a central role in ensuring that Canadians live in safe and secure communities. The Government of Canada is committed to working cooperatively with our provincial/territorial partners, the private sector and the international community to protect the infrastructure and essential services vital to the health and well-being of Canadians, our economy, environment and way of life.

Emergency Management Act

The federal government is taking a big step forward by ensuring that we have a robust legislative framework in place to recognize critical infrastructure protection in the spectrum of emergency management and public safety. Bringing greater accountability to critical infrastructure protection at the federal level, the Minister of Public Safety has introduced the *Emergency Management Act* (EMA), which will modernize the Government's approach to emergency management and align federal roles and responsibilities with today's realities and threat environment.

As part of the EMA, federal ministers will be responsible for identifying risks to critical infrastructure within their respective areas. Moreover, each department or agency will be required to develop emergency plans to address these risks. Each department will maintain, test, and exercise these emergency management plans according to the policies and programs established by the Minister of Public Safety.

On an international scale, the EMA recognizes that the impacts of attacks or disruptions can cascade across borders and sectors. The EMA will enable the Minister of Public Safety, in consultation with the Minister of Foreign Affairs, to coordinate Canada's response to an emergency in the United States, as well as develop joint plans and initiatives.

Information Sharing

Collaboration and information sharing are longstanding traditions connecting the governments of Canada and the U.S., which translates into a common commitment to enhance the security, prosperity and quality of life in both countries. These collaborative traditions are formalized in mechanisms such as the *Security and Prosperity Partnership of North America* (SPP), which provides the framework for both countries to develop common approaches to emergency management, critical infrastructure protection and information sharing.

Government of Canada information sharing practices related to CIP are based on the principles articulated in the *Access to Information Act* (ATIA), which include the public's right to access information held by the Government of Canada along with specific exceptions to that right. The exceptions in the ATIA are similar to those in the U.S. *Freedom of Information Act* (FOIA). For example, when confidential information is provided to the Government of Canada by a foreign government, that information is protected by a specific and mandatory exemption in the *Access to Information Act* (ATIA) and cannot be disclosed.

Building on Canada's current system of safeguards, the *Emergency Management Act* includes consequential amendments to the ATIA that protects specific critical infrastructure/emergency management information shared by private sector owners and operators of Canada's critical infrastructure. This type of information will enable the Government of Canada to develop comprehensive emergency management plans, mitigation and preparedness measures, and to improve warning capabilities and develop better defences and responses, thus helping to bring emergency management into the 21st century. Similar to the United States' FOIA, the ATIA exempts from disclosure any information that is considered important for national security. Exemptions from disclosure for reasons of national security and public safety also exist under provincial jurisdictions.

National Strategy

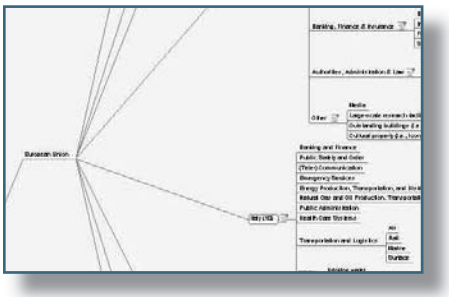
To ensure a higher-level of readiness and effective information sharing, Canadians want all levels of government working together to protect critical infrastructure. Canada's

(Continued on Page 13)

International Definitions of Critical Infrastructure: Summary and Comparison

CIP Program research has resulted in the development of two interactive maps featuring information on critical infrastructure (CI) from an international perspective: 1) international definitions of CI, and 2) international CI sectors. This article offers a brief summary and comparison of the international definitions of CI apparent in research findings to date, representing 11 countries, three international organizations, and one project funded by the European Commission. Six of these 11 countries are Member States of the European Union, which offers its own definition of "European Critical Infrastructure" (ECI).

For the most part, the definitions of CI (offered along with their respective country/organization in the accompanying appendix) are similar. In sum, they overwhelmingly indicate that CI are those infrastructures whose disruption or destruction would result in a serious impact on social and economic well-being and national security. Some definitions use stronger terminology than "serious impact," such as "debilitating impact." Others also include the effective functioning of government in their definitions, which can, in essence, be tied to national security. Further, many definitions expand on social and economic well-being to include public health, safety, and security. The definition used by the North Atlantic Treaty Organisation (NATO) features these two latter additions.



A full version of a map delineating international definitions for critical infrastructure can be found ***here***.

Despite using similar core language, some countries include more detailed factors in their CI definitions, contributing to the argument that not all infrastructure is, or should be deemed, critical. These include the provisions that infrastructure or services are considered critical should they, if disrupted or destroyed:

- be negatively impacted "for an extended period" (Australia);
- affect a "large proportion of the population" (New Zealand);
- "require immediate reinstatement" (New Zealand);
- be "vital to the maintenance of *primary* social and economic processes" (France; emphasis added);
- "cause a sustained shortage of supplies, significant disruptions to public order or other dramatic consequences" (Germany);
- result in "damage on a national scale" (Netherlands); and
- "cause large-scale loss of life[,] . . . have other grave social consequences for the community[, or] be of immediate concern to the national government" (United Kingdom).

Belgium is unique in that it distinguishes CI by one of three types: vital points, sensitive points, and critical points. These types are based on importance, e.g., whether CI are important due to socio-economic factors or to national defense, and on potential threats to persons or groups of people, buildings and facilities, and other assets. Comparatively, a task team of the Organisation for Economic Co-operation and Development (OECD) developed a definition that organizes CI into "social infrastructure" and "economic infrastructure."

The European Union, consisting of 27 Member States, distinguishes ECI from other CI by asserting that any disruption or destruction "would affect two or more Member States or a single Member State if the critical infrastructure is located in another Member State." Put simply, to fall under the category of ECI, impacted CI must affect at least two Member States. The European Union will only step in to assist in adverse situations when assistance is requested by a Member State; the responsibility of CI protection inherently belongs to CI owners and operators and Member States.

This research is continuing and new CIP Program research products are presently being developed.
(Continued on Page 5)

Country / Organization	Definition of Critical Infrastructure
Australia	"Critical infrastructure is defined as 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."
Canada	"Canada's critical infrastructure consists of those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of Canadians or the effective functioning of governments in Canada."
New Zealand	"By critical infrastructure this report means infrastructure necessary to provide critical services. Critical services are those whose interruption would have a serious adverse effect on New Zealand as a whole or on a large proportion of the population, and which would require immediate reinstatement."
Switzerland	"[C]ritical infrastructures . . . are systems and assets whose incapacity or destruction would have a debilitating impact on the national security and the economic and social well-being of a state."
United States	Critical infrastructure are "[a]ssets, systems, and networks, whether physical or virtual, so vital to the United States that the incapacity or destruction of such assets, systems, or networks would have a debilitating impact on security, national economic security, public health or safety, or any combination of those matters." *Note:* The United States often uses the terminology "critical infrastructure and key resources" (CI/KR). "As defined in the Homeland Security Act, 'key resources' are publicly or privately controlled resources essential to the minimal operations of the economy and government."
European Union (EU)	". . . European Critical Infrastructure – that is critical infrastructure that, if disrupted or destroyed, would significantly affect two or more Member States or a single Member State if the critical infrastructure is located in another Member State. With due regard to existing Community competencies, the responsibility for protecting National Critical Infrastructures falls on the NCI owners/operators and on the Member States. The Commission will support the Member States in these efforts only where requested to do so."
Belgium	"Belgium identifies three types of critical infrastructure: vital points, i.e. facilities that require protection because of their socio-economic importance, e.g. nuclear plants, bridges, ports, etc.; sensitive points, i.e. facilities that require protection because of their importance for the national or allied defence potential; critical points, i.e. persons, public authorities, communities, buildings, facilities, places and goods which face a real or potential threat of political or criminal nature."
Finland	Critical Infrastructure to Be Secured: • Technological infrastructure of society • Transportation, logistics and distribution systems • Food supply • Energy supply • Social and health care arrangements • Industry and systems related to national defence
France	"All infrastructures that are vital to the maintenance of primary social and economic processes are considered critical sectors in France."
Germany	"Critical infrastructures (CI) are organisations and facilities of major importance to the community whose failure or impairment would cause a sustained shortage of supplies, significant disruptions to public order or other dramatic consequences."
Netherlands	"[A] sector was deemed 'critical' if its breakdown or serious disruption could lead to damage on a national scale."
United Kingdom	"The [Critical National Infrastructure (CNI)] comprises those assets, services and systems that support the economic, political and social life of the UK whose importance is such that loss could: • cause large-scale loss of life • have a serious impact on the national economy • have other grave social consequences for the community • be of immediate concern to the national government."

(Continued on Page 13)

International Organizations Address CIP

In the past year, several international governments and organizations have generated reports concerning critical infrastructure protection and national security for their respective countries and regions. While each varies in strategy and method, all hold the same objective: to describe governmental approaches to minimizing the negative impacts of terrorism and natural disasters. The following summaries are intended to provide an abbreviated overview of select international reports.

Central Asia Regional Economic Cooperation (CAREC): Regional Cooperation on Disaster Management and Preparedness

In 2006 the Central Asia Regional Economic Cooperation (CAREC) published a paper concerning the importance of disaster management and preparedness. The report concludes that natural disasters in Central Asia could bring catastrophic social and economic consequences to the region, mainly due to a current lack of national and regional disaster preparedness. While limited national and regional policies do exist, Central Asia is still under prepared to handle the potential social and economic devastation.

The authors of the CAREC report suggest that the best way to improve disaster preparedness would be to develop and mainstream national disaster risk management (DRM) systems, as well as encourage regional cooperation alongside DRM. By incorporating disaster risk prevention into national economy and development processes, the authors contend that economic and social losses due to natural disasters would be drastically reduced. In addition, regional cooperation in DRM is a necessary component in managing the aftermath of a disaster and in ensuring that the region is able to maintain economic growth.

Several recommendations for cooperation and risk management for both regional and national implementation are given in the report. Adequate training, public awareness, sharing of resources, and application of existing knowledge are the main objectives of these suggestions for successful disaster prevention and mitigation in Central Asia.

Communication from the Commission on a European Programme for Critical Infrastructure Protection

This communication from the European Commission in December 2006 focuses on the implementation of a European Programme for Critical Infrastructure Protection (EPCIP). The document outlines the means and processes proposed to successfully put into action the EPCIP in order to better protect critical infrastructures in the European Union.

The Commission discusses five measures set in place to help with the implementation and progress of EPCIP.

1) **EPCIP Action Plan:** This plan will serve as a means for the EPCIP to efficiently make progress with respect to fixed deadlines and agendas.

2) **Critical Infrastructure Warning Information Network (CIWIN):** This information network is a means to quickly exchange alerts and warnings in a secure and confidential manner.

3) **Expert Groups:** These groups will be set up in order to support EPCIP by offering analyses and advisories related to CIP.

4) **The CIP Information Sharing Process:** This process allows for the respect and security of privacy rights for different stakeholders who exchange sensitive or confidential CIP information.

5) **Identification of Interdependencies:** All interdependencies of different critical infrastructures will be identified and assessed in order to sufficiently address potential threats and risks.

Contingency planning is cited in the report as a key component for the success of implementing an

(Continued on Page 7)

Int'l Reports *(Cont. from Page 6)*
effective European Programme for Critical Infrastructure Protection. Having a well-planned and informed approach, as well as using the participation and cooperation of national and local authorities, to handle potential disasters and attacks is crucial.

Protecting Australia Against Terrorism 2006

The Australian Government acknowledges the serious threat that terrorism poses and has set forth a counter-terrorism strategy to help protect the nation's people and interests. This 2006 publication serves as an update to the 2004 edition, "Protecting Australia Against Terrorism," and focuses on the government's counter-terrorism strategy. The updated edition is presented in two parts: Part 1 concentrates on describing the strategy behind the Australian Government's national counter-terrorism policy, while Part 2 features the main elements and approach concerning Australia's counter-terrorism capabilities.

Part 1 describes how the Australian Government aims to implement its counter-terrorism strategy by closely working with different levels of government and various sectors. By keeping the Australian public and private sectors informed and involved, the government hopes to strengthen the nation's capabilities of fighting terrorism. The Australian Government also seeks to play a role in more international efforts against terrorism in collaboration with its allies from around the world.

Part 2 explains the capabilities of the Australian Government in fighting terrorism in terms of four aspects: prevention, preparedness, response, and recovery. Preventative measures and preparedness are implemented to assist in deterring terrorist threats, while response and recovery refer to the actions taken in the case of a terrorist incident.

Australia strives to remain ever vigilant by continuously making efforts to strengthen and develop its counter-terrorism strategy for the protection of the nation and communities.

Backgrounder: NATO's Role in Civil Emergency Planning

This report from September 2006 addresses the purpose and benefits of Civil Emergency Planning (CEP) and the role that NATO has taken in contributing to and implementing CEP activities.

Among other things, NATO serves as a means for examining national programs to analyze whether their approaches and procedures are sufficient in the case of an emergency. NATO is able to create the avenue and opportunity for civilian and military authorities to communicate and join forces in an effort to protect their nations. This communication is necessary since the advice and expertise that national authorities are able to offer are vital components in the success and continuation of the NATO operations.

The CEP activities of NATO have been able to aid many ally nations in need. For instance, following Hurricane Katrina in 2005, NATO was able to come to the aid of the United States. In the same year, Pakistan suffered a devastating earthquake after which NATO was able to offer assistance and relief.

In addition to offering relief services, NATO is concerned with international education on critical infrastructure protection. NATO has strived to improve Civil Emergency Planning internationally by promoting the importance of nations' cooperation in sharing pertinent CIP information, as well as taking care to properly educate and train authorities and communities in preventing potential devastation.

For the full text PDF version of these reports please visit the newly updated CIP Library's collection of select international reports at http://cipp.gmu.edu/clib/international.php. ❖

Legal Insights

Quarantine & Isolation

Colleen Hardy
Senior Research Associate , CIP Program

The Department of Defense released its Pandemic Influenza Implementation Plan in May 2007. The report articulated the Department of Defense's roles and responsibilities to protect the nation during an influenza pandemic. One of the main pillars in DoD's plan includes containment. The plan stated that DoD may provide support and transportation, upon direction of the President or approval by the Secretary of Defense, for civilian communities. In addition, the Department of Defense may provide security in support of pharmaceutical and vaccine distribution and they may provide defense assistance for civil disturbances. Lastly, the Department of Defense's Pandemic Influenza Implementation Plan stated that the DoD may assist U.S. civil authorities to enforce a quarantine or an isolation order.

In October 2005 President Bush suggested that military force may be required to enforce quarantines during an influenza pandemic. Later that year, President Bush issued an executive order which added pandemic influenza to the federal list of diseases that can lead to quarantine.

The federal government's authority to issue a quarantine or isolation order is derived from Section 261 of the Public Health Service Act. However, a state's authority to issue a quarantine or isolation order is derived from the state's police power. According to the Center for Disease Control, isolation and quarantine are public health strategies implemented to protect the public by preventing exposure to infected or potentially infected persons. Isolation separates individuals who have a specific infectious illness from individuals who are healthy and restricts the infected individual's movement. On the other hand, quarantine separates and restricts the movement of individuals who are not yet ill, but have been exposed to an infectious agent and thus may become infectious.

The federal government has not issued a federal order of isolation under the Public Service Act since 1963. However, on May 24, 2007 the Center for Disease Control issued an order of isolation for Andrew Speaker. Speaker, a lawyer in Atlanta, Georgia who was aware that he had TB, flew to Europe on May 12. There is a disagreement concerning whether he was told to remain in the United States or not. A health official in Georgia stated that Speaker was informed that he was not highly contagious, rather than not contagious at all. According to Speaker, Fulton County indicated that they preferred him not to travel but he was under the belief that he was not contagious and thus went ahead with his scheduled trip to Europe to get married. The CDC contacted Speaker while he was in Rome and notified him that his drug-resistant form of tuberculosis (XDR-TB) was rarer than they originally believed it to be. In addition, the CDC advised him that he should not travel on an airplane and that his passport was the subject of a no-fly order. Speaker flew to Canada and shortly thereafter, he rented a car and entered the United States on May 24. At this time, the CDC contacted him and he voluntarily entered a hospital in New York. CDC issued a federal order of isolation under the Public Health Service Act. Speaker is currently a patient at the National Jewish Medical Research Center in Denver, Colorado.

In Arizona, another individual has the same drug resistant TB that Speaker has. However, unlike Speaker, Robert Daniels has been in quarantine since last summer. He stayed at a halfway house in Phoenix for indigent TB patients in July 2006 under a voluntary quarantine. The order directed Daniels to continue his medical treatment as well

(Continued on Page 12)

Enhanced CIP Library provides clearinghouse of information

The CIP Program's website (http://cipp.gmu.edu/) is frequently updated, primarily to reflect the ongoing work of the Program and its research staff. Nonetheless, although major documents are often posted to the CIP Library as they become available and a few new pages within the Library were added over the past year, this key area of the CIP Program website has been relatively static. Thanks to a dedicated intern working at the CIP Program this summer, the public will soon see an enhanced CIP Library.

CIP Digital Archive

Beginning last fall, CIP Program staff added the "CIP Digital Archive" to the CIP Library. The contents of the CIP Digital Archive are the culmination of a research project funded by the CIP Program and conducted by George Mason University's Center for History and New Media (CHNM). The CIP Oral History Project ran from July 2003 to the publication of Critical Path, a book that details the history of CIP in the United States, first released in June 2006. An archive of both government and non-government reports, Congressional testimony and hearing transcripts, weblinks, and other relevant information currently comprise the CIP Digital Archive page.

Additional information has been posted to the CIP Program's website to reflect the breadth of the CIP Oral History Project. As part of this information, visitors to the CIP Program website are invited to participate in a survey on their personal experiences with CIP, from policy-making to the handling of incidents affecting critical infrastructure. Survey responses will assist the Program in continually building a historical record of CIP.

Selective Reports Webpages

The CIP Library currently features four "selective reports" webpages:

- Selective Government Reports on Infrastructure Protection;
- Selective Reports on Critical Infrastructure Recovery and Restoration;
- Selective Government Reports on Hurricanes; and
- Selective International Reports and Other Documents.

The last webpage is a recent addition to the CIP Library and will see significant updates this summer. New documents will be posted to the remaining webpages, thus enhancing the overall repository of CIP information that is the CIP Library.

The CIP Library also features webpages on CIP Program-sponsored research publications and projects.

Core CIP Program Research

The Core CIP Program Research webpage (http://cipp.gmu.edu/research/) features research on an array of issues, many of which are supported by documents posted in the CIP Library. Research products available include monographs on resilience and the Committee on Foreign Investment in the U.S. (CFIUS), working papers on relevant legal issues such as the federalization of the National Guard, articles on the war on terrorism, and numerous other written products developed by CIP Program staff. Additionally, interactive maps stemming from research on international critical infrastructure are available for download. Transcripts of "Critical Conversations" and information from other CIP Program-hosted events are also posted to this webpage.

This information adds to core research performed by CIP Program staff, much of which is described in the Projects section of the CIP Program website.

Stay tuned to the CIP Library for continual updates and new information! ❖

Keeping the Key to the Internet from Getting into the Wrong Hands

Symposium explores technical, legal, and political options for securing root zones.

By Christine Pommerening, Ph.D.

When designing technologies and implementing policies aimed at making the Internet more secure, the wide variety in function and functionality of the network usually prevents a one-size-fits-all solution. The occasional online shopper at home has very different needs and capabilities than an army engaged in net-centric warfare. The importance of securing transactions on FedWire cannot be compared to securing those on eBay. But since all of those functions and functionalities are still essentially based on one single infrastructure, a governance framework needs to be found to coordinate those different security needs across the globe.

On May 17, 2007, a symposium organized by GMU's CIP Program, Syracuse University's E-Governance Program, and the Swiss Ecole Polytechnique Fédérale de Lausanne addressed these issues from technical, legal, and political perspectives.

The first panel consisted of representatives from various Internet governance organizations and stakeholders such as IANA and VeriSign, who debated the pros and cons of the DNSSEC (Domain Name System Security Extension). These extensions would add origin authentication and data integrity records to the DNS to detect certain attacks such as spoofing. The principle of DNSSEC is the distribution and use of trusted keys. Zone operators (such as VeriSign for .com) would deploy DNSSEC within their root via signing keys. End users then would update their resolvers to be DNSSEC-compatible by adding so-called anchored keys, which cannot easily be changed or updated. One of the many questions around DNSSEC is who should hold the key signing keys, and thus control access to all root content – the U.S. government who recently reiterated its historic role in authorizing changes or modifications to the root zone file, or ICANN, arguably the most influential Internet governance body to date, or a new consortium of various non-governmental organizations, as suggested by one of the panelists. Handling those keys is not only a significant operational challenge, but raises issues of liability and incident response few stakeholders seem to be willing or able to assume.

The second panel featured legal and policy experts defining the proper role of government and the private sector in global Internet security. The stakes have increased since the Internet has become a vector for everything from military defense to social networking, while we still lack the framework for discerning and acting on threats. Technical problem definitions do not distinguish what needs to be distinguished from an institutional point of view – what is a cyber nuisance, what a criminal intent, what an act of war? For example, the rules of cyber defense are not addressed in the international realm; neither in new Internet-centered institutions such as ICANN, nor in traditional international governmental organizations such as the UN. Nationally, governments must define for themselves what role they have in enhancing security – they can act as regulator, provide incentives, or own and operate their own networks. The private sector has established the IT-ISAC for addressing threats, vulnerabilities, and consequences of cyber attacks based on a flexible organizational model of information sharing. At the same time, their challenge remains to build an operational capacity that matches this governance model.

The last panel addressed the issue of privacy. The WHOIS database epitomizes the need to balance individual rights with collective concerns about discriminating between good and bad actors. Conceptually,
(Continued on Page 14)

...whether the issue is technical, national, or individual security, any Internet governance regime is expected to provide solutions, while preserving the flexibility, autonomy, and sovereignty of the Internet and its stakeholders.

European Network and Information Security Agency (ENISA)

The European Network and Information Security Agency (ENISA) serves as a center of excellence for EU Member States and EU Institutions on network and information security matters.

ENISA's activities are focused on:

1. Advising and assisting the Commission and the Member States on Information Security and addressing security-related problems in hardware and software products in dialogue with industry.
2. Collecting and analyzing data on security incidents and emerging risks in Europe.
3. Promoting risk assessment and risk management methods to enhance our capability to deal with information security threats.
4. Exchange of best practices in awareness-raising and co-operation between different actors in the information security field, notably by developing public / private partnerships with industry in this field.
5. Tracking the development of standards for products and services on Network and Information Society. ❖

ENISA's comments on the recent cyber attack on Estonia

The Agency, as a Centre of Expertise, has no operational role and does not cover fighting cyber crime, since it is not within the mandate of ENISA. (Cybercrime is dealt with by Member State law enforcement authorities and e.g., Europol.) The Agency comments on the cyber attack on Estonia:

Events in Estonia highlight that pro-active security needs the support of Incident Response (IR) capabilities in the moments of crisis. Cyber attacks against Estonia, mainly in the form of Distributed Denial of Service (DDoS) attacks, primarily targeted the Estonian Government and police sites. Private sector banking and on-line media were also heavily targeted and the attacks affected the functioning of the rest of the network infrastructure in Estonia. As a result, the targeted sites were inaccessible outside of Estonia for extended periods in order to subdue the attacks and to maintain services within the country.

DDoS attacks are hard to mitigate and demand a lot of coordination and cooperation from various parties. CERT Estonia, established late last year, along with many local security managers and CERTs from other countries had to establish such a cooperative effort quickly to subdue the attacks. Various CERTs from Europe and beyond helped to involve the international CERT community in mitigating attacks in Estonia.

ENISA has the role to advise the European Bodies (such as the European Commission) and the Member States in NIS issues. As such, it has been promoting various good practices, including CERTs.

Directory and Links to EU CERTs*

*Several EU nations have multiple CERTs. For a full listing, go to http://www.enisa.europa.eu/cert%5Finventory/index_inventory.htm

CERT	Year Est.
RHNet CERT (Iceland)	2003
HEANET CERT (Ireland)	2002
MODCERT (UK)	2001
CERT.PT (Portugal)	2002
CCN CERT (Spain)	2006
CERTA (France)	1999
CERT-IT (Italy)	1994
SWITCH CERT (Switzerland)	1995
BELNET CERT (Belgium)	2004
RU-CERT (Russia)	1998
CERT-FI (Finland)	2002
SITIC (Sweden)	2003
NORCERT (Norway)	2004
CERT ESTONIA	2006
CERTA (France)	1999
LATNET CERT (Latvia)	2006
LINET CERT (Lithuania)	1998
TR-CERT (Turkey)	2003
GRNET-CERT (Greece)	2000
Cyprus CERT	2001
CERT Hungary	2004
ACOnet (Austria)	2003
CESNET CERTS (Czech Rep)	2004
CARNet CERT (Croatia)	2004
CERT POLSKA (Poland)	1996
SI-CERT (Slovenia)	1994

Legal Insights *(Cont. from Page 8)* obtained an involuntary quarantine order for Daniels. He is currently being held in the jail's unit at the county hospital. He has not been charged with a crime but rather is being held under the court order. Daniels admitted that he did not take his medication or wear a mask out in public, however he feels trapped in his current situation. The American Civil Liberties Union filed a suit on behalf of Daniels. The ACLU did not request Daniel's release, but instead requested more humane conditions for Daniels. According to the ACLU, Daniels is not permitted any exercise or fresh air, he has a light on in his hospital room 24 hours a day and has very limited access to television and the telephone.

Both Speaker's and Daniel's cases raise serious public health and legal issues. A Department of Homeland Security official noted that the process to place Speaker on the no-fly list was hampered by discussions between DHS, CDC and Justice Department officials attempting to determine if DHS had the authority to place him on the list. The uncertainty among the officials surfaced due to the fact that the no-fly list is intended to be a counter-terrorism measure. Another issue in Speaker's case concerns the state's authority to prohibit Speaker from flying. According to the director of the CDC, Julie Gerberding, "In Georgia, if a patient is to be isolated in an involuntary manner, it takes a court order and *(Continued on Page 14)*

UK CPNI *(Cont. from Page 2)*
international terrorist threat with its emphasis on suicide tactics, person borne improvised explosive devices, and an aspiration to use CBRN, means that new counter measures are needed, underpinned by a forward-looking research and development programme. In a global and networked world, CPNI also takes a lead role in countering the threat of electronic attack.

CPNI recognises the importance of working internationally and has a positive relationship with the Department of Homeland Security in the U.S. Both the UK and the U.S. recognise the similarities and the common challenges we face, and CPNI and DHS gain considerable benefit from exchanges of information which help to increase the strengths of each country's protective security capability. ❖

CIP Definitions *(Cont. from Page 5)*

Country / Organization	Definition
Assessment for Critical Infrastructure Protection (ACIP)	"The term Large Complex Critical Infrastructure (LCCI) defines a distributed network of independent, mostly privately-owned, man-made systems and processes working collaboratively and synergistically to produce and distribute a continuous flow of essential goods and services. An LCCI is an infrastructure (such as an electric grid, a telecommunications network or a railway/air/road transportation network) whose destruction or degradation can entail severe consequences to public health, safety, security, or the economy."
North Atlantic Treaty Organisation (NATO)	"Critical infrastructure are those assets, facilities, networks and services which, if disrupted or destroyed, would have a serious impact on the health, safety, security, economic well being or effective functioning of a country."
Organisation for Economic Co-operation and Development (OECD)	"The Asian Development Bank (ADB) uses the definition of infrastructure developed by the Task Team on Infrastructure for Poverty Reduction, which distinguishes 'social infrastructure' (such as health, education, and culture) from 'economic infrastructure' (such as transport, energy, information and communication technology, and irrigation, drinking water, and sanitation)."

* The sources of these definitions are found in the notes of the map entitled International Definitions of Critical Infrastructure, available for download at: http://cipp.gmu.edu/research/CriticalInfrastructureMapping.php.

Canada *(Cont. from Page 3)*
national approach is two-fold. First, the draft *National Strategy for Critical Infrastructure Protection* will set out the overarching concepts relevant to all critical infrastructure sectors and jurisdictions. Aligning the activities and challenges of each of the critical infrastructure sectors and each jurisdiction into a coherent roadmap is fundamental to identifying risks, reducing vulnerabilities, conducting research and development, addressing interdependencies and effectively responding to disruptions. Moving forward with this collective approach, the National Strategy will serve as the basis for enhanced collaboration between all levels of government and the private sector and, as such, will remain 'evergreen.'

However, in order to keep pace with the rapidly evolving threat environment, an ongoing state of renewal is required. Therefore, the second element of Canada's national approach is the development of a flexible Action Plan that builds on the central themes of the National Strategy: sustainable partnerships with all levels of government and the private sector, improved information sharing and protection, and a commitment to all-hazards risk management. This Action Plan will be updated on an iterative basis to enable partners to anticipate new risks and adopt new best practices.

Together, the *National Strategy for Critical Infrastructure Protection* and supporting Action Plan, in addition to the *Emergency Management Act*, will establish a collective approach that will be used to set national priorities, goals and requirements for critical infrastructure protection. This collective approach will enable funding and resources to be applied in the most effective manner to reduce vulnerabilities, mitigate threats, and minimize the consequences of attacks and disruptions. ❖

Symposium *(Cont. from Page 10)*
a case can be made for both strong digital identities, and strong privacy protection. If strong digital identities of individuals and groups are developed, decentralized action in favor of or against someone else becomes possible, regardless whether any of the parties involved is public, private, national, or international. If strong privacy protection is implemented, the attack threats may remain, but the consequence to the affected user is minimized. For industry, recent suggestions by the German government to increase business' rights to self-enforce copyright and identity theft might solve some of the third-party problems currently impeding the prosecution of bad actors.

In conclusion, whether the issue is technical, national, or individual security, any Internet governance regime is expected to provide solutions, while preserving the flexibility, autonomy, and sovereignty of the Internet and its stakeholders. This is challenging, but the difficulty to distinguish bad actors in the constantly and rapidly changing online world has always presented a problem for technologists and policymakers alike. In the late 1990s, the problem was separating cyber squatters from legitimate domain name holders. In the early 2000s, it was sorting out spam from personal emails. Today, there is evidence that bad actors may be targeting not only the applications, but the very core of the Internet, i.e. the root zone servers and protocols. Keeping the Internet secure is thus a collective task, while keeping the DNSSEC key, as well as managing other truly critical elements of the infrastructure, may again require a governmental solution. ❖

Legal Insights *(Cont. from Page 12)*
the patient must first demonstrate that he is not compliant with medical advice." Some officials have stated such a law prevents health officials from acting proactively to protect the public. And finally, Daniels' case raises questions about balancing the state's need to protect the public while maintaining an individual's civil liberties. ❖

The CIP Program is directed by John A. McCarthy, a member of the faculty at George Mason University School of Law. The CIP Program works in conjunction with James Madison University and seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems and economic processes supporting the nation's critical infrastructure. The CIP Program is funded by a grant from The National Institute of Standards and Technology (NIST).

The CIP Report is published by Zeichner Risk Analytics, LLC (ZRA) on behalf of the CIP Program. 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/cgi-bin/wa?SUBED1=cipp-report-l&A=1