Critical Infrastructure Protection Education and Training Programs

The mission of critical infrastructure protection (CIP) requires a robust education and training community. Today there are a variety of domestic and international programs that have developed, or are currently developing, curricula that include the examination of critical infrastructure protection. The following list provides a sample of existing CIP degrees, concentrations, courses, and training programs.

Graduate Degree

Master in Strategic Planning for Critical Infrastructures (MSPCI)
The University of Washington College of Built Environments, Department of Urban Design and Planning

The Master in Strategic Planning for Critical Infrastructures is a fully accredited online graduate program that commences each fall. Students "learn to apply strategic planning and decision-making strategies to analyze the vulnerabilities of critical infrastructures; plan responses to failures; and develop resilience." The degree blends education in strategic planning and systems theory, and includes topics such as communications and the legal and ethical issues relevant to homeland security.

In addition to the MSPCI degree, the Department of Urban Design and Planning collaborates with the School of Public Health to develop courses that instruct students about public health and emergency response systems.

For more information about the MSPCI degree, please visit the following website: http://www.outreach.washington.edu/mspci/.

Graduate Concentration

Specialty: *Critical Infrastructure Protection*
Master of Science in Computer Science
Missouri University of Science and Technology

This specialty provides computer science students with an opportunity to specialize in critical infrastructure protection, focusing on vital integrated systems of the nation's critical infrastructures. The intent of this program is to "improve the quality, survivability, security, and reliability of critical systems using the broadest-based technology possible, to grow a workforce aware of and trained in security (physical and cyber), and to stimulate the economic viability of U.S. corporations and institutions by improving the security, reliability, and survivability of their critical infrastructures."

> ***"Missouri S&T's strong emphasis in science and engineering allows us to conduct research and educate students in critical cyber-physical infrastructure protection."***
>
> — Dr. Bruce McMillin, Professor and Graduate Coordinator
> Director of Center for Information Assurance
> Department of Computer Science, Missouri University of Science and Technology

For more information about this program, please visit the following website: http://cs.mst.edu/graduatedegreeprograms/mscomputerscience.html.

Individual Courses

Graduate Course: *Critical Infrastructure Protection of Health Care Delivery Systems*
Master of Homeland Security in Public Health Preparedness
The Pennsylvania State University

Critical Infrastructure Protection of Health Care Delivery Systems examines the operations of health care delivery systems during a natural disaster or terrorist attack, including the disaster's effects on "transport systems, computer and internet security, communications, energy supply, and industry and governmental institutions." The students study the consequences of

(Continued on Page 12)

CIP *(Cont. from 11)*

the disruption of health care delivery systems.

The course is part of the curriculum for the Master of Homeland Security in Public Health Preparedness, an online graduate degree program developed by the Penn State College of Medicine. This program is currently the sole homeland security degree offered by a medical school in the United States. The course is also required for Penn State's online Graduate Certificate in Bioterrorism Preparedness and the online Graduate Certificate in Disaster Preparedness.

For more information about the course and these programs, please visit the following website: http://www.worldcampus.psu.edu/MasterinHomelandSecurity.shtml.

Graduate Course: *Protecting Critical Resources and Infrastructure*
The University of Texas at Dallas School of Economic, Political and Policy Sciences

The *Protecting Critical Resources and Infrastructure* course instructs students about the methods, policies, plans, and innovative technologies that are currently involved in protecting both public and private critical resources and infrastructure. This course requires students to learn various theories of how to respond to threats to infrastructure and assets, as well as how to apply preventative and mitigation measures.

"I believe that homeland security courses such as UT Dallas' Protecting Critical Resources and Infrastructure course are more important than ever to Public Affairs students who will eventually manage organizations that have large amounts of resources and assets that need to be protected from external and internal threats."

— Dr. Nicolas A. Valcik, Associate Director of the Office of Strategic Planning and Analysis and Clinical Assistant Professor Program of Public Affairs, The University of Texas at Dallas

This course is a core requirement for the Graduate Certificate in Homeland Security offered through the Public Affairs Program. In addition, this course may apply towards the Master of Public Affairs, the Master of Science in Criminology, or the Master of Science in International Political Economy.

For more information about this course and the programs offered within the School of Economic, Political and Policy Sciences, please visit the following website: http://epps.utdallas.edu/.

Certificate Course: *Information Assurance and Critical Infrastructure Protection*
Information Assurance Program National Defense University Information Resources Management College

The *Information Assurance and Critical Infrastructure Protection* course focuses on public policy and strategic management. Students will "analyze laws, national strategies, and public policies; and assess the strengths and weaknesses of various approaches for assuring the confidentiality, integrity, and availability of those information assets created, stored, processed, and communicated by information systems and critical information infrastructures."

The course is part of the Information Assurance (IA) Program, which consists of a variety of certificates for information systems security professionals, senior systems managers, risk analysts, and chief information security officers.

For more information about the course and program, please visit the following website: http://www.ndu.edu/irmc/index.htm.

<u>International Training Programs</u>

Protecting Critical Infrastructure Program
ARC Training International Academy for Security Management United Kingdom

The Protecting Critical Infrastructure Program is a five-day training program for security managers who exercise leadership roles in the critical infrastructure

(Continued on Page 16)

Cyber Conflict Perspectives

Ideal Curriculum for International Cyber Incident Management Legal Studies

by Eneken Tikk, M.Jur.

Try to imagine a lawyer who would help you to resolve issues related to cyber incident management. As there is only little time to react, he or she should probably quickly understand the essence of the action and be practical about the recommended steps to take. This is a lot easier said than done, as lawyers must be thorough and base their advice on existing legal and policy frameworks.

Regarding cyber incidents, these frameworks may not always be easily identified or understood. There are different legal areas involved and often the essence of the cyber incident in question first needs to be legally qualified in order to understand in which legal domain the solutions fall. For example, an intrusion into a network may be very disturbing, but not necessarily criminal. It may also be far more serious than just a single criminal intention and fall into the legal notion of terrorist activities. Drawing a line between different concepts and deciding on the application of a specific area of law is a challenging task. A further complicating factor is the inconsistency in terminology regarding cyber incidents, which hinders development of a common policy approach to cyber security.

Not only is it likely that different legal regimes come into play in order to resolve a situation (e.g., basic information security legal requirements for business governance, criminal law or potentially law of armed conflicts), it is also the case that what may be clear in one country, may not be granted in another. While there are countries that have supported in their legislation the quality and availability of logs or the cooperation between national CERTs, etc., there are other countries that have little or no regulation on cyber security and jurisdictions. Also, since there are different national authorities and processes involved, the same legal provision may be differently implemented in different countries.

This all makes resolving an internationally relevant cyber incident quite difficult. And it is even more difficult to find a lawyer who could understand all the different legal regimes involved and practices implemented. Therefore, an ideal curriculum of cyber incident management legal issues would, first of all, give lawyers a basic understanding of the technical environment of their work — the technologies, basics of cyber security management, and relevant policies and strategies. Then, it would cover the legal aspects of daily cyber security to support lawyers' orientation in the practical aspects of preventing network intrusions or information leaks.

Naturally, the curriculum would touch upon the criminal policy and law in the field, indicating not only what has been agreed upon at the international level in terms of prohibited activities and practical criminal cooperation, but also covering individual country practices in implementing different international agreements and policy documents. It would address the unique features of cybercrime and the difficulties in solving the cases (such as no borders in cyber space, identification issues, jurisdiction problems, etc.). It would also provide the background required to debate policy issues such as "do we need a cyber terrorism treaty?" and "what do we actually mean by that?"

Also, the curriculum would indicate other perspectives of cyber incident resolution and relevant risk assessments, involving concerns of military, diplomats, intelligence, business and policy experts. Such a curriculum would also include discussion of new concepts of law,

(Continued on Page 15)

Infrastructure Protection Education and Risk Management

Panel Discussion, including:

- Barbara Yagerman, DHS Office of Infrastructure Protection, Partnership and Outreach Division.
- Ed Jopeck, Director and Immediate Past President of SARMA.
- Will McGill, Penn State University, Assistant Professor of Information Sciences and Technology.
- Maeve Dion, CIP Program Manager, Education and Cyber.

Part of the 3rd Annual Security Analysis and Risk Management Association (SARMA) Conference at the Arlington campus of George Mason University, in partnership with the Center for Infrastructure Protection (CIP) at the George Mason University School of Law.

Conference features confirmed Keynote Speakers:

- Mr. Peter F. Verga, Deputy Under Secretary of Defense for Policy Integration and Chief of Staff to the Under Secretary of Defense for Policy

- Ms. Tina Gabbrielli, Director of the Office of Risk Management and Analysis, U.S. Department of Homeland Security

- Mr. Roger W. Cressey, President of the Good Harbor Consulting Group and former Director for Transnational Threats on the National Security Council.

16 - 18 June 2009

Agenda and registration information available on the event website.

EMPP-CIP *(Cont. from 2)*

Saturdays, in addition to two multiple-day residencies.

As a public policy program, EMPP-CIP combines perspectives on business and government, law and economics, culture and technology while emphasizing critical infrastructure protection and resilience. The EMPP-CIP concentrates not only on administration but also on management and judgment as these relate to policy formulation and implementation.

Executive Education

The EMPP program is the newest addition to the extensive range of program options offered by the George Mason University School of Public Policy (SPP). Currently offering five Master's degrees and a Ph.D. in Public Policy, SPP attracts nearly 1,000 students from the U.S. and abroad, and has one of the largest public policy doctoral programs in the country. In addition to degree programs, the School conducts short-term professional development programs for corporate and government executives and organizes frequent public forums.

With its 70 full-time teaching and research faculty, 30 high-level adjunct teaching faculty, and nearly 40 professional staff, SPP maintains twelve research centers, and external research support averages more than $8 million a year, making it the number one program in its field for federal and total research expenditures as ranked by the National Science Foundation. ❖

For more information on the EMPP-CIP, contact Christine Pommerening cpommere@gmu.edu.

Perspectives *(Cont. from 13)*

policy, international coordination, etc.

Finally, an ideal curriculum would look at the most severe cases where cyber incidents may involve political or coercive motivation and involve nation states as targets or initiators and discuss how much of the law of armed conflict is applicable to cyber incidents. It would look at strategic and tactical offensive and defensive aspects of information operations (IO) by state and non-state actors to achieve political, military, and economic goals through IO means.

An ideal is likely never quite real. But after some research, it seems that it is not so difficult to imagine a master's program that would offer all these perspectives. There are a number of universities in the United States, Europe and elsewhere that have established LL.M. programs to educate law students in practical aspects of cyber conflict and whose programs, although somewhat differently focused, could be integrated into a holistic approach to what a legal cyber response team needs to have as their background knowledge.

The Center for Infrastructure Protection has started working on the details of an ideal curriculum that would provide national and international lawyers from industry, government, and academia with the "big picture" of cyber conflict and therefore help them meaningfully approach the issues brought up by their employers, without losing track of where their solutions fit into in a wider perspective. We

(Continued on Page 17)

CIP *(Cont. from 12)*

protection sectors. Samples of critical infrastructure protection issues that are included in the training curriculum include: defining critical infrastructure; assessing current threats; analyzing risk and vulnerability assessment methodologies; establishing baseline security criteria; emergency planning; and examination of specific sectors such as transportation, energy, water, and agriculture.

For more information about this training program, please view the following website: http://www.arc-tc.com/pages/index.asp.

Critical Infrastructure Awareness
Advanced Distributed Learning Course
The Partnership for Peace Consortium of Defense Academies and Security Studies Institutes

Created at the behest of the NATO Conference of Commandants of Alliance Defense Colleges, the course is a Canadian product offered for use by NATO members and Partners. This course is intended for current and prospective strategic-level decision makers (civilian and military) who wish to enhance their knowledge and awareness of critical infrastructure protection. The course emphasizes European examples of critical infrastructure protection.

"The Canadian Defence Academy provided the technical and instructional design expertise for the course development." Other members of the development team included subject matter experts from the Canadian Forces College and the Public Safety and Emergency Preparedness Canada (PSEPC), recognized experts in the critical infrastructure protection field. ❖

Course History:

"In 2002, the NATO Conference of Commandants agreed to examine the question whether or not Critical Infrastructure Protection would be a suitable subject to be taught at Defence Colleges. The Canadian Forces College (CFC) Commandant at the time, Brigadier General Gagnon, agreed to lead a coalition of the willing to examine the question. Thirteen countries partook in a working group led by CFC which identified the objectives and teaching points."

— LCdr (RET) Robert Charest, Deputy Manager of the Project

For more information about this course, please click here.

ERM *(Cont. from 3)*

associations, the American Public Power Association and the National Rural Electric Cooperative Association, in identifying and building audiences for the training. ❖

For further information about this project, contact the program director, Dr. Brien Benson, George Mason University, 703-993-3171, bbenson@gmu.edu.

Manual *(Cont. from 8)*

not receive PCII protections.

As you read this Manual, you may have questions regarding PCII Program procedures. Please do not hesitate to contact us at pcii-info@dhs.gov or (202) 360-3023. We welcome your feedback and are glad to discuss how PCII protections may be applied to information shared with the Federal government. ❖

For more information on the PCII program, please visit: http://www.dhs.gov/PCII.

Perspectives *(Cont. from 15)*

welcome involvement by any and all subject matter experts who are interested in this effort. Please contact Eneken Tikk or Maeve Dion. ❖

CAPTAP *(Cont. from 10)*

available to help with regional CIP efforts.

DHS IP is planning to make this an annual conference; check the Web page below for conference announcements. ❖

For More Information

Visit IP's CAPTAP Web page on DHS.gov for a more detailed description of the program (http://www.dhs.gov/xinfoshare/programs/gc_1195679577314.shtm).

To learn more about C/ACAMS, e-mail the C/ACAMS Project Office at ACAMS-info@hq.dhs.gov, call 703–235–3939, or visit: http://www.dhs.gov/acams.

The Center for Infrastructure Protection works in conjunction with James Madison Univerity 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 Center is funded by a grant from the National Institute of Standards and Technology (NIST).

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