**Course Number: XXXX**

**Critical Infrastructure Security and Resilience: The International Dimension**

**University of XXXXXX**

**Fall/Spring Semester 20XX**

**name of school:**

**department:**

**program:**

**professor:**

Telephone Number:

Office Location:

Office Hours:

Email:

Website:

**course description/overview:**

The security and resilience of critical infrastructure within the United States is a complex topic that requires consideration of the international dimension. The global economy, global risk environment, global supply chain, cross-border infrastructures, and multi-national corporate entities are elements of this multi-dimensional reality of the 21st century. From an operating perspective, critical infrastructure sectors and systems are increasingly interdependent and vulnerable due to the nature of their physical environments, functionality, supply chains, and cyber interconnections. The ever-evolving threat environment affecting our critical infrastructures comprises a diverse and complex mix of manmade and naturally occurring threats and hazards. In the face of such risks, governments at the national and multi-national levels and international corporations have developed various approaches to secure and enhance the resilience of critical infrastructures and supply chains. Although approaches may vary by country, by region and by infrastructure sector, the majority attempt to achieve a balance of resilience and risk-informed prevention, protection, and preparedness activities to more effectively mitigate current and future risk.

This course will provide an in-depth, comparative look at these issues and the dynamic interplay between the various stakeholders engaged in the critical infrastructure security and resilience mission area internationally.

This course is a 15-lesson graduate-level elective seminar providing a focus on critical infrastructure security and resilience from the international perspective. It is designed to promote subject-matter understanding, critical analysis of complex, multi-dimensional issues, comparative insight into various frameworks and approaches, and an appreciation of the constantly changing dynamics of the critical infrastructure risk and operating environments. Specific areas of focus include a comparative look at: government-private sector policy approaches; governance/organizing structures; partnerships and information sharing; incident management mechanisms; best-practices for risk assessment, risk management, and performance measurement; methodology for managing cyber risks; infrastructure and supply chain dependencies and interdependencies; and the future infrastructure risk and operating environments. The course also features a comprehensive practical examination of critical infrastructure sector stakeholder interaction and key subject-matter areas through in-class group exercises and activities and a learner research report and oral presentation. These “hands-on” applications will reinforce knowledge and critical thinking skills gained throughout the course and help learners fully recognize the “no-man-is -an-island” nature of critical infrastructure security and resilience in an international context.

The course begins with a brief review of the evolution of critical infrastructure security and resilience as a major international policy area, including an overview of the representative policies, strategies, frameworks, and plans that provide national- and multi-national level guidance for this subject area. The course then turns to an examination of the authorities, roles, and responsibilities of governments and the private sector in accordance with various national and multi-national approaches. The course next examines the various “building blocks” of critical infrastructure security and resilience: public-private partnerships, information sharing, and risk assessment and management, with examples of each provided in the context of various national and multi-national operating models. This discussion sets the stage for the next section of the course in which learners will assess, compare, and contrast the various international approaches to critical infrastructure security and resilience through three individual case studies focusing on: the United States-Canada partnership, the European approach (European Union, United Kingdom, and NATO models), and Pacific Basin models. The course next will examine various international approaches to cyber security and supply chain security, with a focus on the nature of critical dependencies and interdependencies across infrastructure sectors and national borders. The course will conclude with an examination of the challenges related to the future critical infrastructure risk and operating environments.

**credits conferred:** 3

**prerequisite:** None

**learner outcomes/objectives (as aligned to the u.s. department of homeland security (dhs) critical infrastructure core competencies):**

This course is designed to enable learners to:

**1. Recognize critical infrastructure security and resilience as a key international policy area**:

* Define the term “critical infrastructure” and identify international factors that must be considered to ensure security and resilience.
* Examine the evolution of critical infrastructure security and resilience as a national and multi-national policy focus area.
* Provide an introduction to different overarching policy approaches and organizing constructs in use internationally and facilitate discussion of implications for policy making today.
* Examine the various definitions of “critical infrastructure” and “resilience” and national, bi-national, and multi-national-level sector constructs as applied in the international context.
* Examine how the global risk environment has affected national and multi-national approaches to critical infrastructure security and resilience over time.

**2. Identify and assess the various authorities, roles, and responsibilities related to critical infrastructure security and resilience at the national and multi-national levels.**

* Examine the roles and responsibilities of government and the private sector in the context of various critical infrastructure security and resilience regimes.
* Examine the various governance structures in use internationally to organize a collaborative, public-private approach to critical infrastructure security and resilience.
* Discuss the principal political, organizational, legal, and resource challenges that those responsible for critical infrastructure security and resilience face in executing those responsibilities.

**3. Identify and assess the various organizing constructs, partnerships, and information sharing processes and systems in place to support the critical infrastructure security and resilience mission internationally:**

* Understand the key factors that underpin the need for public-private partnerships and information sharing in the international context.
* Discuss the relationship between critical infrastructure and the global economy.
* Discuss the role of international corporations and cross-border infrastructure.
* Evaluate the impacts of disruptions to infrastructure within the United States, to infrastructures outside the United States, and vice versa.
* Discuss how critical infrastructure security and resilience-related information is collected, warehoused, protected, and exchanged between government and the private sector in the context of various national and multi-national information sharing models.
* Discuss processes and considerations for cross-border or international information sharing.
* Explain the ongoing challenges to information sharing and collaboration that exist internationally.

**4. Explain how the 21st century risk environment applies to the critical infrastructure security and resilience mission area:**

* Threats: terrorism, cyber attacks, natural disasters and naturally occurring phenomena (e,g. pandemics), industrial accidents and other manmade events, and other emergencies
* Vulnerabilities (facility, node, and system level).
* Consequences (public health and safety, economic loss/disruption, continuity of government and essential services, iconic loss, etc.).
* Dependencies/interdependencies.

**5. Compare and contrast different national and multi-national strategic approaches and issues regarding critical infrastructure risk assessment, risk management, and performance measurement:**

* Develop an understanding of the major elements of risk (threats, vulnerabilities and consequences) in the context of international critical infrastructure security and resilience.
* Examine the challenges associated with critical infrastructure security and resilience in the current and projected threat/hazard environment.
* Explore how various nations and multi-national entities calculate critical infrastructure risk and/or formally assess the risk to critical infrastructure.
* Examine the various regulatory and voluntary approaches to critical infrastructure security and resilience in use internationally.
* Explain the concept of resilience and its application to the critical infrastructure arena, both in the United Stated and internationally.
* Identify and discuss various critical infrastructure risk management initiatives underway internationally, with an eye toward “best-practice” solutions.

**6. Using a case study approach, analyze and be able to discuss various national, bi-national, and multinational approaches to critical infrastructure security and resilience.**

* Assess the following in the context of specific case studies:
	+ public-private partnerships
	+ information sharing
	+ risk assessment & management
	+ planning
	+ incident management
* Compare/contrast the United States approach with other models for critical infrastructure security and resilience in use internationally.

**7. Discuss the “borderless” nature of the cyber threats and challenges that impact the critical infrastructure security and resilience mission area internationally.**

* Examine the international linkages between cybersecurity and critical infrastructure security and resilience from a strategic and operational perspective.
* Examine the authorities/capacities/resources landscape of the cyber domain as applied to international critical infrastructure security and resilience.
* Explain how cyber risk is assessed and managed internationally within and across the various critical infrastructure sectors.
* Examine the various national and multilateral approaches used to secure the cyber components of critical infrastructure systems internationally, including the variance in cyber standards from country to country.

**8. Examine how dependencies, interdependencies, and supply chain issues impact critical infrastructure risk assessment and management on a global scale.**

* Provide an understanding of the “borderless nature” of dependencies/interdependency and supply chain related issues.
* Explore how critical infrastructure sectors such as energy, transportation, and communications approach the issue of dependencies/interdependencies, including cross-sector cyber security risks and supply chain risks.
* Identify the major elements of effective supply chain strategies and concepts
* Compare and contrast various national, bi-national and multinational approaches to global supply chain security.

**9. Evaluate the complexities associated with international critical infrastructure security and resilience in a dynamic risk and future operating environment:**

* Characterize and discuss the potential future international critical infrastructure security and resilience operational and risk environments and related challenges.
* Assess the potential impacts of issues such as global climate change, aging populations, decaying infrastructures, dependencies and interdependencies, and ever more consequential natural disasters.
* Discuss strategic choices that may impact our approach to international critical infrastructure security and resilience and supply chain security in the medium-long term future (10-20 years from now).

**delivery method:**

Course delivery will include lectures, interactive classroom discussions, in-class exercises, guest speakers, independent research, and a research paper. The assigned course readings include a variety of resources, such as authoritative readings (legislation, executive orders, policies, and plans and strategies), implementation readings (government products that are responsive or attempt to fulfill the requirements of authoritative documents), and external reviews (U.S. Government Accountability Office (GAO), Congressional Research Service (CRS), etc.).

Learners are expected to familiarize themselves with the assigned topic and readings before class and should be prepared to discuss and debate them critically as well as analyze them for biases, particularly the external reviews, and from multiple perspectives. The instructor will facilitate the discussion by asking different levels of questioning (factual, analytical, and application of the material) to evaluate the depth of the learner’s comprehension of the content.

**general course requirements:**

1. Class attendance is both important and required. If, due to an emergency, you will not be in class, you must contact your instructor via phone or email. Learners with more than two absences may drop a letter grade or lose course credit.
2. It is expected that assignments will be turned in on time (the beginning of the class in which they are due). However, it is recognized that learners occasionally have serious problems that prevent work completion. If such a dilemma arises, please speak to the instructor in a timely fashion.
3. The completion of all readings assigned for the course is assumed. Since class will be structured around discussion and small group activities, it is critical for you to keep up with the readings and to participate in class discussion.
4. All electronic devices should be turned off before class begins.

**grading:**

Class Participation (Including In-Class Exercise Activities) 40%

Research Paper 40%

Research Paper Presentation 20%

**activities, exercise, and research projects:**

**1. Research Paper/Oral Presentation (60%)**

Each learner will prepare a 15-20 page research paper on an international critical infrastructure security and resilience issue of their choice. The paper should be organized using the following format: problem statement, background (including key players, authorities, resources, genesis/context of the issue, etc.), discussion (including presentation of the issue, problem areas, alternative solutions and associated pros and cons for each alternative solution), and recommendations. The recommendations section should clearly describe the rationale for the policy option or solution of choice. The research paper also should focus on the benefits, drawbacks, and obstacles to the practical application of the proposed recommendations. Examples of research paper topics include, but are not limited to, the following:

* Alternative approaches to international supply chain security
* Sector-specific approaches to international critical infrastructure security and resilience
* International information sharing for critical infrastructure security and resilience
* International standards and regulations for critical infrastructure security and resilience
* Addressing transnational threats and hazards to critical infrastructure systems
* Building international partnerships for critical infrastructure security and resilience
* Critical infrastructure incident management in an international context
* Bilateral/multilateral approaches to critical infrastructure security and resilience

As an alternative to a research paper, learners may submit a 15-page, section-by-section critique of a national (non-United States) or multi-national level critical infrastructure security and resilience strategy or plan or agreement. Critiques should be structured according to the following basic building blocks: 1) Authorities, 2) Partnering and Information Sharing, 3) Assessing Risk, 4) Managing Risk (regulatory vs. non-regulatory), and 5) All-hazards Management. The critique should include alternative visions/strategies for successful critical infrastructure security and resilience program implementation within the national, bi-national, or multinational framework under study.

Each learner will present his/her research topic or critical analysis (no more than 25-30 minutes in length) to the class on Lesson 13 or 14. The oral presentation format will follow the outline used to develop the research paper/critique. **Research papers will be submitted electronically to the instructor prior to class on Lesson 14.**

Prior approval of the topic for the research paper is required. **Learners** **should submit a one-page written description of their proposed topic to the instructor in class or via email for approval no later than the beginning of class in Lesson 4. Learners may subsequently change their proposed topic with prior approval of the instructor.**

**3. Expectations for Participation (40%):**

Participation includes coming to class prepared, participating in class discussion, and dynamic role playing during in-class exercise activities.

**incorporation of feedback:**

The course instructor will offer multiple opportunities for learners to provide constructive feedback over the period of the course. These feedback channels may take the form of group sessions or one-on-one sessions with the instructor. Learners will be afforded the opportunity to complete mid-term evaluations at the end of Lesson 6, following the conclusion of the scheduled in-class group exercise activities, and at the end of the course. On-line correspondence with the instructor to gain clarity on a specific lesson topic or reference material is also encouraged throughout the course. Finally, the instructor will provide written feedback to the learners on their classroom participation, course research paper and oral presentation at the end of the course. Ongoing dialogue with the instructor regarding in-class exercise preparation, research paper development, and oral presentation preparation is highly encouraged.

**course reading materials:**

There are no primary textbooks assigned for this course. All assigned course reading materials, additional recommended readings, and other references are available online, with website access information provided in the lesson description sections that follow below.

**additional resources (optional):**

Critical Infrastructure Resource Center: <http://training.fema.gov/EMIWeb/IS/is860a/CIRC/index.htm>

International CIIP Handbook (2008-2009), <http://www.css.ethz.ch/publications/pdfs/CIIP-HB-08-09.pdf> or <https://www.hsdl.org/hslog/?q=node/4413>.

U.S. Department of Homeland Security Office of Infrastructure Protection: <http://www.dhs.gov/xabout/structure/gc_1185203138955.shtm>

U.S. Department of Homeland Security Daily Open Source Infrastructure Report: <http://www.dhs.gov/files/programs/editorial_0542.shtm>

Homeland Security Digital Library: <http://www.hsdl.org/>

*The International Journal of Critical Infrastructures*: <http://www.inderscience.com/browse/index.php?journalID=58>

*The CIP Report*: <http://cip.gmu.edu/the-cip-report>

*Homeland Security Affairs*: <http://www.hsaj.org/>

*The Journal of Homeland Security and Emergency Management*: <http://www.bepress.com/jhsem/>

*The Journal of Homeland Security*: http://www.homelandsecurity.org/journal

*The Journal of Homeland Security Education*: [www.JournalHSE.org](http://www.JournalHSE.org)

*The Journal of Infrastructure Systems* (log-in required)

<http://ascelibrary.org/journal/jitse4>

*The European Journal of Transport and Infrastructure Research*: <http://www.ejtir.tbm.tudelft.nl/index.asp>

*The International Journal of Sustainable Transportation*: <http://www.tandf.co.uk/journals/titles/15568318.asp>

*The Journal of Transportation Law, Logistics & Policy*: <http://www.atlp.org/journal.html>

*The International Journal of Logistics Management*: <http://www.emeraldinsight.com/products/journals/journals.htm?id=ijlm>

*The International Journal of Electrical Power & Energy Systems*: <http://www.journals.elsevier.com/international-journal-of-electrical-power-and-energy-systems/>

The Global Homeland Security Education Network: <http://www.northumbria.ac.uk/sd/academic/sass/about/socscience/solscres/interdiscnetworks/ghsen/>

**grading scale (school policy dependent):**

**course lesson descriptions**

**lesson 1 topic: the fundamentals of critical infrastructure Security and resilience in an international context**

**1. Lesson Goals/Objectives:**

* Review the scope of the course, administrative requirements, instructional methodology, reading materials, evaluation criteria, and feedback processes.
* Review the evolution of critical infrastructure security and resilience as a major policy focus area for the United States.
* Examine the evolution of critical infrastructure security and resilience as a major policy focus area for other countries and multinational entities.
* Examine the various definitions of “critical infrastructure” and sector constructs as applied in the international context.
* Examine how the global economy and global risk environment have affected national and multi-national approaches to critical infrastructure security and resilience over time.
* Identify and discuss the various national and multi-national authorities that support international collaboration in the critical infrastructure security and resilience policy arena.
* Discuss the notion of critical infrastructure dependencies & interdependencies and global supply chains as a growing concern internationally.

**2. Discussion Topics:**

* How does the United States define “critical infrastructure?”
* What is meant by cascading effects? How do international considerations factor into this discussion?
* What are the major pillars of the United States approach to critical infrastructure security and resilience? How are these woven into strategy and policy at the national level?
* How has critical infrastructure security and resilience evolved over time as a major policy focus area for the United States? For other countries and multi-national entities such as the European Union? For global corporations and industry?
* How do other countries and multinational organizations define “critical infrastructure?” How do these definitions compare to the United States definitions? Are there implications that can arise from differing definitions or approaches?
* Do other countries use a sector-focused construct, and, if so, how does it differ from the United States approach? What are the major concepts behind critical infrastructure security and resilience in the non-U.S. context?
* Discuss some of the various national and multi-national authorities that support international collaboration in the critical infrastructure security and resilience policy arena.
* How have changes in the global economy and global risk environment affected national and multi-national approaches to critical infrastructure security and resilience over time?
* Why does critical infrastructure security and resilience represent such a challenging policy focus area, both nationally and internationally?
* How have growing concerns over cyber vulnerabilities impacted national and multi-national approaches to critical infrastructure security and resilience?
* Define critical infrastructure dependencies and interdependencies and identify potential impacts that can arise from the global supply chain perspective. Why is this a consideration for the security and resilience of critical infrastructure in the United States? (i.e., why do we care and what can happen if we do not pay attention to what is going on internationally?)

**3. Required Reading:**

*United States:*

Kathi Ann Brown, *Critical Path: A Brief History of Critical Infrastructure Protection in the United States*, Chapters 1-4, 8 and 9. http://cip.gmu.edu/archive/CIPHS\_CriticalPath.pdf

John D. Moteff, *Critical Infrastructure Protection: Background, Policy and Implementation*, 2014, <http://www.fas.org/sgp/crs/homesec/RL30153.pdf>.

Presidential Policy Directive-21: Critical Infrastructure Security and Resilience, February 12, 2013,

<http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.

Executive Order 13636, Improving Critical Infrastructure Cybersecurity, February 12, 2013, <http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf>.

U.S. Department of Homeland Security. *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*, pp. 1-10, 13-14, <http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508.pdf>.

National Infrastructure Advisory Council, *A Framework for Establishing Critical Infrastructure Resilience Goals: Final Report and Recommendations,* (October 19, 2010), <http://www.dhs.gov/xlibrary/assets/niac/niac-a-framework-for-establishing-critical-infrastructure-resilience-goals-2010-10-19.pdf>.

*International:*

Organization of Economic Development, *Protection of ‘Critical Infrastructure’ and the Role of Investment Policies,* (May 2008),

<http://www.oecd.org/daf/inv/investment-policy/40700392.pdf>

Center for Security Studies, *Crisis Risk Network Focal Report 1: Critical Infrastructure Protection,* (October 2008),

<http://www.bevoelkerungsschutz.admin.ch/internet/bs/de/home/themen/ski/publikationen_ski.parsys.71944.DownloadFile.tmp/focalreport1.pdf>

Europa, *Summaries of EU Legislation: Critical Infrastructure Protection,* <http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33259_en.htm>

Harry Hoverd, *International Cooperation on Critical Infrastructure Protection,* (February 2006)

<https://www3.cepol.europa.eu/dspace/bitstream/123456789/376/1/Ausgabe02-06_Art3-Hoverd.pdf>

George Mason University, The Center for Infrastructure Protection and Homeland Security (CIP/HS), *The CIP Report*, 8(1), (July 2009), <http://tuscany.gmu.edu/centers/cip/cip.gmu.edu/wp-content/uploads/2013/06/CIPHS_TheCIPReport_July2009_InternationalCIP1.pdf>.

George Mason University, The Center for Infrastructure Protection and Homeland Security (CIP/HS), *The CIP Report*, 8(12), (June 2010), <http://tuscany.gmu.edu/centers/cip/cip.gmu.edu/wp-content/uploads/2013/06/CIPHS_TheCIPReport_June2010_InternationalCIP.pdf>.

George Mason University, The Center for Infrastructure Protection and Homeland Security (CIP/HS), *The CIP Report*, 9(12), (June 2011),

<http://tuscany.gmu.edu/centers/cip/cip.gmu.edu/wp-content/uploads/2013/06/CIPHS_TheCIPReport_June2011_InternationalCIP.pdf>.

Arjen Boin, Mark Rhinard, and Magnus Ekengren,

*Institutionalizing Homeland Security Cooperation in Europe*,(2007), <http://citation.allacademic.com/meta/p_mla_apa_research_citation/2/1/0/1/5/pages210155/p210155-1.php>.

**4. Additional Recommended Reading:**

*General:*

Philip Auerswald, Lewis M. Branscomb, Todd M. LaPorte and Erwann Michel-Kerjan, *The Challenge of Protecting Critical Infrastructure,* (2005), <http://opim.wharton.upenn.edu/risk/downloads/05-11-EMK.pdf>.

*United States:*

Robert T. Marsh*, Critical Foundations: Protecting America’s Infrastructures*,(1997), <http://www.fas.org/sgp/library/pccip.pdf>.

*Presidential Decision Directive-63, Critical Infrastructure Protection*, (1998), <http://www.fas.org/irp/offdocs/pdd/pdd-63.htm>.

Critical Infrastructure Information Act of 2002, <http://www.dhs.gov/xlibrary/assets/CII_Act.pdf>.

Homeland Security Presidential Directive-7,

*Critical Infrastructure Identification, Prioritization and Protection*, (2003), <http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm#1>.

U.S. Department of Homeland Security, *Quadrennial Homeland Security Review, 2014*, <http://www.dhs.gov/sites/default/files/publications/qhsr/2014-QHSR.pdf>.

*International:*

International Relations and Security Network, *CIP Handbook 2008/9,* (September 2008),

<http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?lng=en&id=91952>

**lesson 2 topic: roles, responsibilities, and governance frameworks**

**1. Lesson Goals/Objectives:**

* Analyze the opportunities and challenges to critical infrastructure security and resilience based on existing authorities, policies, regulations, and approaches used within the United States and other countries.
* Examine the opportunities and challenges for critical infrastructure security and resilience that stem from the established and perceived roles and responsibilities of government and the private sector within the United States and other countries.
* Examine the various governance structures in use internationally to organize a collaborative, public-private approach to critical infrastructure security and resilience.
* Compare and contrast regulated and voluntary critical infrastructure security and resilience regimes internationally across the critical sectors.
* Explain the roles that multi-national corporations and other multi-national entities play in critical infrastructure security and resilience.
* Discuss the principal political, organizational, legal, and resource challenges that those responsible for critical infrastructure security and resilience face in executing those responsibilities.

**2. Discussion Topics:**

* Compare and contrast the various authorities related to critical infrastructure security and resilience at the national, bi-national, and multi-national levels.
* How are goals and objectives regarding the critical infrastructure mission established under the various authorities examined in this lesson?
* Discuss the various governance structures in use internationally to organize a collaborative, public-private approach to critical infrastructure security and resilience.
* What are the key roles and responsibilities of the following with respect to critical infrastructure security and resilience: national governments, multi-national governments, state/provincial governments; the private sector; and nongovernmental organizations? What is the role of the State Department and other Federal departments and agencies?
* How do the various government and private entities with critical infrastructure responsibilities at different levels interact and collaborate with one another? With cross-border and international counterparts?
* Evaluate the various governance structures examined in this lesson to identify effective practices.
* How does the distributed structure of critical infrastructure responsibility and accountability play out against the principal threats faced by nation-states, the private sector, non-governmental organizations, and multi-national entities?

**3. Required Reading:**

*United States*

Presidential Policy Directive-21: Critical Infrastructure Security and Resilience, February 12, 2013,

<http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.

U.S. Department of Homeland Security. *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*, pp. 10-12, Appendix B, 2013, <http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508.pdf>.

Ken Schnepf, *Council Aims to Coordinate State/local Security Efforts*, (2007), <http://www.plantservices.com/articles/2007/198.html>.

Peter R. Orszag, *Critical Infrastructure Protection and the Private Sector: The Crucial Role of Incentives,* Congressional Testimony, (2003), <http://www.brookings.edu/~/media/Files/rc/testimonies/2003/0904healthcare_orszag/20030904.pdf>.

Sue Eckert, *Protecting Critical Infrastructure: The Role of the Private Sector*, (2006), <http://www.ridgway.pitt.edu/LinkClick.aspx?fileticket=Bezaq7AdjxA%3D&tabid=233>.

National Infrastructure Advisory Council, *Critical Infrastructure Partnership Strategic Assessment: Final Report and Recommendations*, (October 14, 2008), <http://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_protection_assessment_final_report.pdf>.

United States House of Representatives, *DHS Cybersecurity: Roles and Responsibilities to Protect the Nation’s Critical Infrastructure,* (March 13, 2013),

<https://www.hsdl.org/?view&did=733614>

*International*

Jennifer Giroux, *Early Warning and Information Sharing in Critical Infrastructure Protection,*

[www.tisp.org/index.cfm?pk=download&pid=10261&id=12603](http://www.tisp.org/index.cfm?pk=download&pid=10261&id=12603)

Angela Gendron, *Critical Infrastructure Protection and Emergency Preparedness in Multi-Jurisdictional Systems: The United Kingdom and the European Union,* (2006), <http://www3.carleton.ca/cciss/res_docs/ceip/gendron.pdf>

Commonwealth of Australia, *National Guidelines for Protecting Critical Infrastructure from Terrorists,* (2011),

[http://www.nationalsecurity.gov.au/agd/WWW/rwpattach.nsf/VAP/(689F2CCBD6DC263C912FB74B15BE8285)~Protecting+Critical+Infrastructure+from+Terrorism+PDF.pdf/$file/Protecting+Critical+Infrastructure+from+Terrorism+PDF.pdf](http://www.nationalsecurity.gov.au/agd/WWW/rwpattach.nsf/VAP/%28689F2CCBD6DC263C912FB74B15BE8285%29~Protecting%2BCritical%2BInfrastructure%2Bfrom%2BTerrorism%2BPDF.pdf/%24file/Protecting%2BCritical%2BInfrastructure%2Bfrom%2BTerrorism%2BPDF.pdf)

NATO Parliamentary Assembly, *The Protection of Critical Infrastructures,* (2007), <http://www.nato-pa.int/default.asp?SHORTCUT=1165>

Bernard Haemmerli and Andre Renda, *Protecting Critical Infrastructure in the EU*, (December 2010),

<http://www.ceps.eu/book/protecting-critical-infrastructure-eu>

European Commission, *Commission Staff Working Document on Review of European Programme for Critical Infrastructure Protection (EPCIP),* (June 22, 2012),

<http://ec.europa.eu/dgs/home-affairs/pdf/policies/crisis_and_terrorism/epcip_swd_2012_190_final.pdf>

Center for Security Studies, *Crisis Response Network Focal Report 2: Critical Infrastructure Protection,* (March 2009),

<http://www.css.ethz.ch/publications/pdfs/Focal-Report-2-CIP.pdf>

**4. Additional Recommended Reading:**

*United States*

U.S. Government Accountability Office, *Influenza Pandemic: Opportunities Exist to Address Critical Infrastructure Protection Challenges That Require Federal and Private Sector Coordination*,(2007), <http://www.gao.gov/new.items/d0836.pdf>.

U.S. Government Accounting Office, *Internet Infrastructure: Challenges in Developing a Public/Private Recovery Plan,* (October 2007), <http://www.gao.gov/new.items/d08212t.pdf>.

**lesson 3 topic: organizing, partnering, and information sharing**

**1. Lesson Goals/Objectives:**

* Understand the key factors and concepts that underpin public-private information sharing in the international context.
* Identify the principal types and sources of information that support the critical infrastructure security and resilience mission within the United States and internationally.
* How does the global nature of many companies impact critical infrastructure information sharing?
* Identify and discuss the partnership structures, processes, and coordinating mechanisms integral to the U.S. National Infrastructure Protection Plan (NIPP) Partnership Model.
* Deconstruct the nature of collaborative interaction among the Sector Coordinating Councils, Government Coordinating Councils, and Regional Consortium Coordinating Councils under the United States model.
* Identify and discuss the government-industry authorities, structures, processes, and coordinating mechanisms utilized in the other national and multi-national critical infrastructure partnership frameworks presented in this lesson.
* Discuss how critical infrastructure security and resilience-related information is collected, warehoused, protected, and exchanged between government and the private sector in the various international information sharing models presented in this lesson.
* Explain the limitations to and ongoing challenges and barriers to information sharing and collaboration that exist between government and the private sector in the context of the United States, Canadian, European Union, and Australian critical infrastructure security and resilience frameworks.

**2. Discussion Topics:**

* What are the key motivations that drive government-private information sharing for critical infrastructure security and resilience? Are these motivators the same in both the U.S. context and internationally?
* What are the key elements of the NIPP Partnership Model utilized in the U.S. context? How do the various elements of the NIPP Partnership Model interact with one another?
* What are the key processes and systems used to share critical infrastructure data, to include intelligence information, among the various NIPP stakeholders nationally, regionally, and locally?
* How do the partnership structures, processes, and coordinating mechanisms utilized in other national and multi-national critical infrastructure partnership frameworks differ from the U.S. model?
* How is critical infrastructure-related information collected, warehoused, protected, and exchanged between government and the private sector in the various international information sharing models presented in this lesson?
* What are the challenges associated with information sharing within a multi-national entity such as the EU?
* How is classified national security information shared between government and industry in the U.S. model and internationally?
* How and from whom does the private sector receive terrorism-related information?
* What are the principal barriers to all-hazards information sharing between government and the private sector within the U.S. context and internationally?
* How does information sharing contribute to incident management regarding borderless infrastructure systems?
* Do any of the models presented in this lesson represent a “best-practice” for critical infrastructure partnerships and information sharing? Why or why not?

**3. Required Reading:**

*United States*

U.S. Department of Homeland Security. *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*, Appendix A, <http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508.pdf>.

U.S. Department of Homeland Security, *Critical Infrastructure protection Partnerships and Information Sharing,*

<http://www.dhs.gov/critical-infrastructure-protection-partnerships-and-information-sharing>

National Infrastructure Advisory Council, *Critical Infrastructure Partnership Strategic Assessment: Final Report and Recommendations*, (October 14, 2008), <http://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_protection_assessment_final_report.pdf>.

*Information Sharing Environment*,<http://itlaw.wikia.com/wiki/Information_Sharing_Environment>.

*The Role of ISACs in Private/Public Sector CIP*, (2009),

<http://www.surfacetransportationisac.org/SupDocs/Library/ISAC_Products/isac_role_in_cip.pdf>.

*Information Sharing and the Private Sector*,[*http://www.ise.gov/sharing-private-sector*](http://www.ise.gov/sharing-private-sector).

National Association of Regulatory Utility Commissioners, *Information Sharing Practices in Regulated Critical Infrastructure States*, (June 2007),

<http://www.naruc.org/Publications/NARUC%20CIP%20Information%20FIN.pdf>

Robert Riegle, Testimony, *The Future of Fusion Centers: Potential Promise and Dangers*, (2009), <http://www.dhs.gov/ynews/testimony/testimony_1238597287040.shtm>.

George Mason University, The Center for Infrastructure Protection and Homeland Security, *The CIP Report*, 11(10), (April 2013), <http://tuscany.gmu.edu/centers/cip/cip.gmu.edu/wp-content/uploads/2013/06/April2013_PartershipsInformationSharing.pdf>.

*International*

UNICRI, *Public-Private Partnerships (PPPs) for the Protection of Vulnerable targets against Terrorist Attacks: Review of Activities and Findings,* (January 2009), <http://www.un.org/terrorism/pdfs/Web-Protecting%20Human%20Rights.pdf>

The 2012 Critical Infrastructure Symposium: *Early Warning & Information Sharing in Critical Infrastructure Protection (CIP)*,Jennifer Giroux, Senior Researcher and Project Manager, Risk & Resilience Research Group, Center for Security Studies, ETH Zurich, <http://www.tisp.org/index.cfm?pid=12506&&stCode=live&preview=yes&cdid=12508>.

EUR-lex, *Communication from the Commission on a European Programme for Critical Infrastructure Protection,* (2006),

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52006DC0786:EN:NOT>

Federal Ministry of the Interior, Federal Republic of Germany, *Protection of Critical Infrastructures*, (2013), <http://www.bmi.bund.de/EN/Themen/Europa/Sicherheit/Kritis/kritis_node.html>

**Bruce Richardson, Eleanor Hill, Phyllis Summer, Pulina Whitaker and Alexander Haas, *Cybersecurity Efforts to Secure Critical Infrastructure including the Energy Sector Advance in the United States and European Union,* (2013),**

<http://www.kslaw.com/library/newsletters/EnergyNewsletter/2013/March/article1.html>

Euroalert.net, *European Critical Infrastructure Warning Information Network,* (April 2013), <http://euroalert.net/en/news.aspx?idn=8037>

Ludek Lukas and Martin Hromada, *Perspective of Information Support of CR Critical Infrastructure Protection,*

<http://www.wseas.us/e-library/conferences/2012/Paris/DEEE/DEEE-39.pdf>

Public Safety Canada, *National Strategy for Critical Infrastructure*, (2010),

<http://www.publicsafety.gc.ca/prg/ns/ci/ntnl-eng.aspx>

Office of the Auditor General of Canada, *2009 March Status Report of the Auditor General of Canada, Chapter 1 - National Security: Intelligence and Information Sharing,* (March 2009), <http://www.oag-bvg.gc.ca/internet/English/parl_oag_200903_01_e_32288.html>

Government of Australia, *Trusted Information Sharing Network (TISN) for Critical Infrastructure Resilience,* <http://www.tisn.gov.au/Pages/default.aspx>

**4. Recommend Additional Reading:**

*United States*

*A Policy Framework for the ISAC Community*,(2004),

<http://www.isaccouncil.org/images/Policy_Framework_for_ISAC_Community_013104.pdf>.

Critical Infrastructure Resource Center, *Partnerships*,

<http://training.fema.gov/EMIWeb/IS/is860a/CIRC/index.htm>.

Homeland Security: Protecting, Analyzing & Sharing Information, <http://www.dhs.gov/topic/information-sharing>.

*National Strategy for Information Sharing*, (2007),

<http://georgewbush-whitehouse.archives.gov/nsc/infosharing/index.html>

**lesson 4 topic: identifying and assessing critical infrastructure risk**

**\*\*special activity: research paper topic descriptions due.**

**1. Lesson Goals/Objectives:**

* Identify the major elements of risk (threats, vulnerabilities and consequences) and understand how various nations and multi-national entities calculate critical infrastructure risk and/or formally assess the risk to critical infrastructure.
* Identify and discuss the various threats (including the evolving terrorist threat) and hazards that may impact critical infrastructure within and across the different sectors in both the U.S context and internationally.
* Examine the challenges associated with critical infrastructure security and resilience in the current and projected threat/hazard environment.

**2. Discussion Topics:**

* What are the major elements of risk as they pertain to the critical infrastructure?
* In the current environment, how would you identify the greatest threats to critical infrastructure? Are these threats the same in the U.S. as in other countries? What are the impacts or ramifications of the similarities or differences?
* How do the human, physical, and cyber dimensions of critical infrastructure security and resilience relate to the concept of risk in the international context?
* How does the U.S. calculate critical infrastructure risk? How is critical infrastructure risk assessed outside the U.S.? What are the major commonalities among the various approaches employed? Differences?
* How does the U.S. calculate risk related to critical infrastructure dependencies/interdependencies? How is such risk assessed outside the U.S.? What are the major commonalities among the various approaches used? Differences?
* Is there an international “best practice” or potential standard for critical infrastructure risk assessment?
* How do multi-national entities come to common terms regarding the assessment of critical infrastructure risk that crosses national boundaries?
* How does critical infrastructure risk inform strategic decisions, national security policy, planning, and resource investments in the U.S. model? From the perspective of other nations/multi-national entities?

**3. Required Reading:**

*General*

Georgios Giannopoulos, Roberto Filippini, and Muriel Schimmer**,** *Risk Assessment Methodologies for Critical Infrastructure Protection. Part I: A State of the Art, (2012),*

<http://ec.europa.eu/home-affairs/doc_centre/terrorism/docs/RA-ver2.pdf>

*United States*

Congressional Research Service, *What Makes Infrastructure Critical?* (2002),

<http://www.libertysecurity.org/IMG/pdf/CRS_Report_-_What_makes_an_Infrastructure_Critical_-_30.08.2002.pdf>.

U.S. Department of Homeland Security. *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*, pp. 15-20,

<http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508.pdf>

George Mason University, The Center for Infrastructure Protection and Homeland Security, *Critical Infrastructure Protection: Elements of Risk*,Various articles, (2007),

<http://cip.gmu.edu/wp-content/uploads/2014/03/ElementsofRiskMonograph.pdf>.

Committee to Review the Department of Homeland Security's Approach to Risk Analysis, National Research Council, *Review of the Department of Homeland Security's Approach to Risk Analysis*, (2010), <http://download.nap.edu/cart/deliver.cgi?record_id=12972>.

Brian Jackson and David Frelinger, *Emerging Threats and Security Planning*,(2009), <http://www.rand.org/pubs/occasional_papers/2009/RAND_OP256.pdf>.

Congressional Research Service Report, *International Terrorism and Transnational Crime: Security Threats, U.S. Policy, and Considerations for Congress*, (March 18, 2010),

<http://assets.opencrs.com/rpts/R41004_20100318.pdf>.

U.S. Government Accountability Office, *DHS List of Priority Assets Needs to Be Validated and Reported to Congress*, (March 2013), <http://www.gao.gov/assets/660/653300.pdf>

The 2012 Critical Infrastructure Symposium: *Lessons Learned from Past Attacks on America’s Infrastructure*,Raymond H. Bennett, Ph.D., P.E., Baker Engineering and Risk Consultants Inc., <http://www.tisp.org/index.cfm?cdid=12461&pid=10261>

*International*

Infrastructure Canada,

*Literature Review of Methodology to Evaluate the State of Infrastructure*, (August 2007), <http://www.worldcat.org/title/literature-review-of-methodology-to-evaluate-the-state-of-infrastructure/oclc/311303097>

C. Di Mauro, S. Bouchon, M. Atkinson, J.P. Nordvik, G. Spadoni, and G. Antonioni, *Towards Risk assessment of Critical Infrastructures: Experience Gained from Quasi-Real Time Vulnerability Assessment of the Transportation of Dangerous Substances by Road*, <http://conference.ing.unipi.it/vgr2006/archivio/Archivio/2006/Articoli/700173.pdf>

Bart Smedts, *Critical Infrastructure Protection at the European Level,* (2011),

<http://www.nonproliferation.eu/documents/other/bartsmedts4ec14cdd011bd.pdf>

Rand Corporation, *The Lessons of Mumbai*, (2008), <http://www.rand.org/pubs/occasional_papers/2009/RAND_OP249.pdf>.

NATO Parliamentary Assembly, *The Protection of Critical Infrastructures,* (2007),

<http://www.nato-pa.int/default.asp?SHORTCUT=1165>

Public Safety Canada, *Action Plan for Critical Infrastructure,* (2010), <http://www.publicsafety.gc.ca/prg/ns/ci/ct-pln-eng.aspx#aE>

Government of Australia, *Critical Infrastructure Resilience Strategy,* (2010),

[http://www.tisn.gov.au/Documents/Australian+Government+s+Critical+Infrastructure+Resilience+Strategy.pdf](http://www.tisn.gov.au/Documents/Australian%2BGovernment%2Bs%2BCritical%2BInfrastructure%2BResilience%2BStrategy.pdf)

**4. recommended additional reading:**

*United States*

DHS Risk Lexicon, <http://www.fema.gov/pdf/government/grant/2011/fy11_hsgp_lexicon.pdf>.

Robert A. Miller and Irving Lachow, National Defense University, *Strategic Fragility: Infrastructure Protection and National Security in the Information Age*,(2008), <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA476034&Location=U2&doc=GetTRDoc.pdf>.

**lesson 5 topic: managing critical infrastructure risk**

**1. Lesson Goals/Objectives:**

* Explain the concept of resilience and its application to the critical infrastructure arena, both in the U.S. and internationally.
* Examine the various national and multi-national perspectives on critical infrastructure risk management.
* Identify and discuss the various regulatory and voluntary approaches to critical infrastructure and resilience in use internationally.
* Identify and discuss how different nations and multi-national entities manage the risks related to critical infrastructure dependencies/interdependencies.
* Identify and discuss the challenges associated with the management of critical infrastructure risk and performance measurement at the national and multi-national levels.
* Identify and discuss various critical infrastructure risk management initiatives underway internationally, with an eye toward “best-practice” solutions.

**2. Discussion Topics:**

* Compare and contrast the various national and multi-national perspectives on critical infrastructure risk management. Is there an approach that stands out as a best practice? Why or why not?
* Do the various national and international approaches to critical infrastructure security and resilience presented in today’s lesson rely on regulatory measures? Voluntary measures? A combination thereof?
* Why is a regulatory approach favored in some national/international models?
* How do the various national and international approaches to critical infrastructure security and resilience presented in today’s lesson deal with the issue of dependencies/interdependencies?
* How does the concept of “resilience” apply to critical infrastructure security and resilience in an international context? How does the U.S. define resilience? Other nations/multi-national entities?
* Is the concept of “resilience” equivalent to “business continuity” from the perspective of global corporations? Why or why not?
* Are “security” and “resilience” mutually exclusive concepts? How do other nations/multi-national entities “blend” the two concepts?
* Is there a difference between how government and industry tend to view the concept of resilience, both in the U.S. and internationally?
* What are the major recommendations of the 2009 National Infrastructure Advisory Council (NIAC) Report regarding resilience? Do you concur with them? If not, what would be your recommendation? Could these recommendations be applied internationally?

**3. Required Reading:**

*General*

Philip Auerswald, Lewis M. Branscomb, Todd LaPorte, and Erwann Michel-Kerjan,

*The Challenge of Protecting Critical Infrastructure*,(2005), <http://opim.wharton.upenn.edu/risk/downloads/05-11-EMK.pdf>.

Dr. Jim Kennedy, *Critical Infrastructure Protection is all about Operational Resilience*, (2006), <http://www.continuitycentral.com/feature0413.htm>.

T.D. O’Rourke, *Critical Infrastructure, Interdependencies and Resilience,* (Spring 2007),

<http://www.nae.edu/File.aspx?id=7405>.

Brian Jackson, *Marrying Prevention and Resiliency*, (2008), <http://www.rand.org/pubs/occasional_papers/2008/RAND_OP236.pdf>.

*United States*

U.S. Department of Homeland Security. *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*, pp. 15-20,

<http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508.pdf>

American Society of Civil Engineers, *Guiding Principles for the Nation’s Critical Infrastructure,* (2009)

<http://content.asce.org/files/pdf/GuidingPrinciplesFinalReport.pdf>

U.S. Government Accountability Office, *Critical Infrastructure Protection: DHS Has Taken Action Designed to Identify and Address Overlaps and Gaps in Critical Infrastructure Security Activities*,(May 19, 2011),<http://www.gao.gov/new.items/d11537r.pdf>.

National Infrastructure Advisory Council, *Optimization of Resources for Mitigation of Infrastructure Disruption Study Final Report and Recommendations,* (October 19, 2010), <http://www.dhs.gov/xlibrary/assets/niac/niac-optimization-resources-final-report-10192010.pdf>.

*International*

Patrick Lagadec, *Critical Infrastructures and Governance: New Frontiers, New Visions, New Partnerships,* (2003),

<http://www.patricklagadec.net/fr/pdf/suede.pdf>

Public Safety Canada, *Risk Management Guide for Critical Infrastructure Sectors,* (2010), <http://www.publicsafety.gc.ca/prg/ns/ci/_fl/rmgcis-ggrsie-eng.pdf>

Federal Ministry of the Interior, Federal republic of Germany, *Protecting Critical Infrastructures –Risk and Crisis Management: A Guide for Companies and Government Authorities,* (2008),

<http://www.bmi.bund.de/SharedDocs/Downloads/EN/Broschueren/Leitfaden_Schutz_kritischer_Infrastrukturen_en.pdf?__blob=publicationFile>

# Christer Pursiainen*, The Challenges for European Critical Infrastructure Protection,* (2009), <http://www.tandfonline.com/doi/abs/10.1080/07036330903199846?journalCode=geui20#preview>

European Commission, *Commission Staff Working Document on Review of European Programme for Critical Infrastructure Protection (EPCIP),* (June 22, 2012),

<http://ec.europa.eu/dgs/home-affairs/pdf/policies/crisis_and_terrorism/epcip_swd_2012_190_final.pdf>

Adrian V. Gheorghe, *Critical Infrastructures: The Need for International*

*Risk Governance,*

<http://www.nextgenerationinfrastructures.eu/download.php?field=document&itemID=449529>

United Kingdom cabinet Office, *Keeping the Country Running: Natural Hazards and Infrastructure,* (October 2011),

<https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/78900/summary-consultation-responses.pdf>

Government of Australia, *Critical Infrastructure Resilience Strategy,* (2010),

[http://www.tisn.gov.au/Documents/Australian+Government+s+Critical+Infrastructure+Resilience+Strategy.pdf](http://www.tisn.gov.au/Documents/Australian%2BGovernment%2Bs%2BCritical%2BInfrastructure%2BResilience%2BStrategy.pdf)

**4. Additional Recommended Readings:**

*United States*

National Infrastructure Advisory Council,

*Critical Infrastructure Resilience Final Report and Recommendations*,(September 2009),

<http://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_resilience.pdf>.

George Mason University, The Center for Infrastructure Protection and Homeland Security, *The CIP Report*, 12(7), (January 2014), <http://cip.gmu.edu/wp-content/uploads/2013/06/January-2014_Resilience.pdf>.

**lesson 6 topic: case studies: the u.s.-canada critical infrastructure partnership**

**1. Lesson Goals/Objectives:**

* Discuss the Canadian approach to critical infrastructure security and resilience, including:
	+ public-private partnerships
	+ information sharing
	+ risk assessment & management
	+ planning
	+ incident management
* Examine the cross-border implications for critical infrastructure operations, security, and resilience between Canada and the United States.
* Describe border implications and challenges faced by critical infrastructure owners and operators and how they are addressed by private industry. (Examples for discussion can include energy, transportation, critical manufacturing, and others.)
* Discuss the major elements of the North American Electric Reliability Corporation (NERC) framework regarding the resilience and stability of the North American power grid.
* Discuss the major elements of the *Canada-United States Action Plan for Critical Infrastructure* bilateral framework*.*
* Identify and discuss processes used by the United States and Canada to address cross-border infrastructure dependencies/interdependencies.
* Compare and contrast the United States and Canadian approaches to critical infrastructure security and resilience.

**2. Discussion Topics:**

* What are the major elements of *Canada’s National Strategy and Action Plan for Critical Infrastructure*? How is this approach similar to/different from the United States model? Does the Canadian approach offer any seeming best practices?
* Does the North American Free Trade Agreement (NAFTA) play a part in bilateral/trilateral critical infrastructure security and resilience? Should it?
* How is critical infrastructure risk managed at the provincial level in Canada? Are the national and provincial frameworks compatible?
* What is the Canadian perspective on critical infrastructure risk? How is this perspective different from that of the United States?
* What are the major elements of the *Canada-United States Action Plan for Critical Infrastructure* bilateral framework? What are the strengths and weaknesses of this approach?
* Do the United States and Canada use comparable approaches to identify, assess, and manage risk related to cross-border infrastructure systems? If not, how is cross-border infrastructure risk accounted for?
* Discuss the various critiques of *Canada’s National Strategy and Action Plan for Critical Infrastructure?* Are these critiques similar to those associated with the U.S. model?
* How does the NERC framework support the protection and resilience of the North American power grid? What are its principal strengths and weaknesses?
* Does this model have potential applicability to other important cross-border infrastructures?

**3. Required Reading:**

Office of Critical Infrastructure Protection and Emergency Preparedness, Government of Canada, *Threats to Canada’s Critical Infrastructure*, (March 12, 2003),

<http://www.publicsafety.gc.ca/prg/em/ccirc/_fl/ta03-001-eng.pdf>

Public Safety Canada, *National Strategy for Critical Infrastructure and Action Plan for Critical Infrastructure*, (2010), http://www.dhs.gov/xlibrary/assets/ip\_canada\_us\_action\_plan.pdf.

Kevin Quigley, “Man plans, God laughs”: Canada's National Strategy for Protecting Critical Infrastructure,

<http://onlinelibrary.wiley.com/doi/10.1111/capa.12007/abstract>

## *The McDonald-Laurier Institute, Canada’s Critical Infrastructure: Vulnerable to Terrorists, Hackers, Thieves and Neglect,* (December 6, 2011),<http://www.macdonaldlaurier.ca/mli-paper-canadas-critical-infrastructure-vulnerable-to-terrorists-hackers-thieves-and-neglect/>

Troy Media, *Canada’s Critical Infrastructure: When is Safe enough?* (December 16, 2011), <http://www.troymedia.com/2011/12/16/canadas-critical-infrastructure-when-is-safe-safe-enough-part-6/>

Ontario Ministry of Safety and Correctional Services Website, *Critical Infrastructure,* <http://www.emergencymanagementontario.ca/english/emcommunity/ProvincialPrograms/ci/ci.html>

U.S. Department of Homeland Security and Public Safety Canada, *Canada-United States Action Plan for Critical Infrastructure*, (2010),

<http://www.dhs.gov/xlibrary/assets/ip_canada_us_action_plan.pdf>.

North American Electric Reliability Corporation Website,

<http://www.nerc.com/page.php?cid=6%7C69>

Angela Gendron, *Critical Infrastructure Protection in Canada*, (December 2010),

<http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA535390>

The McDonald-Laurier Institute, *Solutions to Critical Infrastructure Problems,*

<http://www.macdonaldlaurier.ca/files/pdf/Solutions-to-Critical-infrastructure-Problems-February-2012.pdf>

**Additional Recommended Reading**

Public Safety Canada, *Critical Infrastructure Partners,* <http://www.publicsafety.gc.ca/prg/ns/ci/prtn-eng.aspx>

Infrastructure Canada, [www.infrastructure.gc.ca](http://www.infrastructure.gc.ca)

**lesson 7 topic: european models: the united kingdom (uk), european union (eu), and north Atlantic treaty organization (nato)**

**1. Lesson Goals/Objectives:**

* Examine the evolution of critical infrastructure security and resilience as a core focus area within the European context.
* Articulate the overall UK, EU, and NATO approaches to critical infrastructure security and resilience, including:
	+ public-private partnerships
	+ information sharing
	+ risk assessment & management
	+ planning
	+ incident management
* Assess the issue of risks to critical infrastructure from a national and multinational perspective in the European context.
* Explain the major elements of the UK Strategy for Critical Infrastructure Protection (CIP) and the various EU directives on critical infrastructure*.*
* Explain how the different national-level approaches are linked to the multinational CIP mandates prescribed in the various EU directives.
* Compare and contrast the United States and European approaches to critical infrastructure security and resilience.
* Explain how the security and resilience of Energy Sector critical infrastructure are addressed in the European context, nationally and internationally.

**2. Discussion Topics:**

* How has the European perspective on critical infrastructure security and resilience evolved over the past decade?
* How do the UK, EU, and NATO approaches to critical infrastructure security and resilience address the following building blocks?
	+ public-private partnerships
	+ information sharing
	+ risk assessment & management
	+ planning
	+ incident management
* How is the issue of risks to critical infrastructure viewed from a national and multinational perspective in the European context?
* What are the major elements of the UK Strategy for Critical Infrastructure Protection (CIP) and the various EU directives on critical infrastructure? How do they differ? How are they similar?
* How are the various national-level approaches followed by individual European countries linked to the multinational CIP mandates prescribed in the various EU directives? Are they mutually supportive?
* How do the various European approaches to critical infrastructure security and resilience differ from the U.S. model? What are the respective strengths and weaknesses of each approach?
* How is the protection and resilience of Energy Sector critical infrastructure addressed in the European context, nationally and internationally?

**3. Required Reading:**

Europa Summaries of EU Legislation, *Critical Infrastructure* *Protection,*

<http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33259_en.htm>

Europa Summaries of EU Legislation, *Critical Infrastructure* *Protection,*

<http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33260_en.htm>

EUR-lex, *Communication from the Commission on a European Programme for Critical Infrastructure Protection,* (2006),

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF>

Europa Press Releases, The European Programme for Critical Infrastructure Protection (EPCIP), (December 12, 2006), <http://europa.eu/rapid/press-release_MEMO-06-477_en.htm>

Council of the European Union, *Council Directive 2008/114/EC:* *Identification and Designation of European Critical Infrastructure and the Assessment of the Need to Improve their Protection*,

<http://www.euractiv.com/en/security/critical-infrastructure/article-140597>.

Europa Summaries of EU Legislation, *European Critical Infrastructures,*

<http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/jl0013_en.htm>

European Commission, *Commission Staff Working Document on Review of European Programme for Critical Infrastructure Protection (EPCIP),* (June 22, 2012),

<http://ec.europa.eu/dgs/home-affairs/pdf/policies/crisis_and_terrorism/epcip_swd_2012_190_final.pdf>

Royal High Institute for Defence Center for Security and Defence Studies, *Critical Infrastructure Protection Policy in the EU: State of the Art and Evolution in the (Near) Future,* (June 2010),

<http://www.irsd.be/website/media/Files/Focus%20Paper/FP15.pdf>

Bernard Haemmerli and Andre Renda, *Protecting Critical Infrastructure in the EU*, (December 2010),

<http://www.ceps.eu/book/protecting-critical-infrastructure-eu>

European Commission Website, Critical Infrastructure Protection,

<http://ec.europa.eu/energy/infrastructure/critical_en.htm>

Angela Gendron, *Critical Infrastructure Protection and Emergency Preparedness in Multi-Jurisdictional Systems: The United Kingdom and the European Union,* (2006),

<http://www3.carleton.ca/cciss/res_docs/ceip/gendron.pdf>

Bart Smedts, *Critical Infrastructure Protection at the European Level,* (2011),

<http://www.nonproliferation.eu/documents/other/bartsmedts4ec14cdd011bd.pdf>

NATO Parliamentary Assembly, *The Protection of Critical Infrastructures*,(2007),

<http://www.Nato-pa.int/default.asp?CAT2=1159&CAT1=16&CAT0=2&com=1165&MOD=0&SMD=0&SSMD=0&STA=0&ID=0&PAR=0&PRINT=1>.

Harry Hoverd, *International Cooperation on Critical Infrastructure Protection,* (February 2006),

<https://www3.cepol.europa.eu/dspace/bitstream/123456789/376/1/Ausgabe02-06_Art3-Hoverd.pdf>

The Scottish Government*, Secure and Resilient: A Strategic Framework for Critical National Infrastructure in Scotland,* (2011), <http://www.epcollege.com/EPC/media/MediaLibrary/Knowledge%20Hub%20Documents/A%20Strategic%20Framework/Secure-Resilient.pdf?ext=.pdf>

Center for Security Studies, *Crisis Risk Network Focal Report 1: Critical Infrastructure Protection,* (October 2008),

<http://www.bevoelkerungsschutz.admin.ch/internet/bs/de/home/themen/ski/publikationen_ski.parsys.71944.DownloadFile.tmp/focalreport1.pdf>

Institution of Civil Engineers, *The State of the Nation: Defending Critical Infrastructure,*

<http://www.ice.org.uk/getattachment/5e93aedd-3b4c-44db-acfa-d176e0ccbb0e/State-of-the-Nation--Defending-Critical-Infrastruc.aspx>

1. **Recommended Additional Reading:**

Center for the Protection of National Infrastructure, <http://www.cpni.gov.uk/>.

Arjen Boin, Mark Rhinard, and Magnus Ekengren,

*Institutionalizing Homeland Security Cooperation in Europe*,(2007), <http://citation.allacademic.com/meta/p_mla_apa_research_citation/2/1/0/1/5/pages210155/p210155-1.php>

**lesson 8 topic: pacific basin models**

**1. Lesson Goals/Objectives:**

* Explain the evolution of critical infrastructure security and resilience as a core focus area within the Pacific Basin context.
* Evaluate the approaches to critical infrastructure security and resilience utilized nationally and multi-nationally across the Pacific Basin, including:
	+ public-private partnerships
	+ information sharing
	+ risk assessment & management
	+ planning
	+ incident management
* Assess the issue of risks to critical infrastructure from a national and multinational perspective in the Pacific Basin context.
* Describe the major elements of Australia’s Strategy for Critical Infrastructure Protection*.*
* Compare/contrast Pacific Basin approaches to critical infrastructure security and resilience to those utilized by the U.S. and EU.
* Explain how the security and resilience of Energy Sector critical infrastructure are addressed in the Pacific Basin context, nationally and multi-nationally.

**2. Discussion Topics:**

* How has the Pacific Basin perspective on critical infrastructure security evolved over the past decade?
* How do the various national and multinational approaches to critical infrastructure security and resilience utilized across the Pacific Basin address the following building blocks?
	+ public-private partnerships
	+ information sharing
	+ risk assessment & management
	+ planning
	+ incident management
* How is the issue of risks to critical infrastructure viewed from a national and multinational perspective within the Pacific Basin context?
* What are the key elements major elements of Australia’s Strategy for Critical Infrastructure Protection? How do they differ from the U.S. approach? How are they similar? Does the Australian model offer any significant best practices for an organization and partnering/risk assessment and management perspective?
* How are the various approaches to critical infrastructure security and resilience utilized in the Pacific Basin different from the EU model? Is there a strong, multilateral approach across the Pacific Basin?
* How do the various Pacific Basin approaches to critical infrastructure security and resilience differ from the U.S. model? What are the respective strengths and weaknesses of each approach?
* How is the protection and resilience of Energy Sector critical infrastructure addressed in the Pacific context, nationally and multi-nationally?

**3. Required Reading:**

## Non-traditional Security Studies’ Blog, *ASEAN’s Critical Infrastructure and Pandemic Preparedness*, (January 22, 2013), <http://ntsblog.wordpress.com/2013/01/22/aseans-critical-infrastructure-and-pandemic-preparedness/>

## Katsuhisa Furukawa, *U.S.-Japan Security Cooperation for Homeland Security: The Cases of Critical Infrastructure Protection and Counter-Bio-Terrorism*, (February 2004),<http://www.strategycenter.net/research/pubID.6/pub_detail.asp>

APEC Website, *APEC Adopts Strategy for Securing Commerce in the Asia-Pacific Region,*

<http://www.apec.org/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Task-Groups/Counter-Terrorism-Task-Force/Secure-Trade-Factsheet.aspx>

Critical Infrastructure Protection Website (Australia),

<http://www.tisn.gov.au/Pages/default.aspx>

Commonwealth of Australia, *National Guidelines for Protecting Critical Infrastructure from Terrorists,* (2011),

[http://www.nationalsecurity.gov.au/agd/WWW/rwpattach.nsf/VAP/(689F2CCBD6DC263C912FB74B15BE8285)~Protecting+Critical+Infrastructure+from+Terrorism+PDF.pdf/$file/Protecting+Critical+Infrastructure+from+Terrorism+PDF.pdf](http://www.nationalsecurity.gov.au/agd/WWW/rwpattach.nsf/VAP/%28689F2CCBD6DC263C912FB74B15BE8285%29~Protecting%2BCritical%2BInfrastructure%2Bfrom%2BTerrorism%2BPDF.pdf/%24file/Protecting%2BCritical%2BInfrastructure%2Bfrom%2BTerrorism%2BPDF.pdf)

Government of Australia, *Critical Infrastructure Resilience Strategy,* (2010),

[http://www.tisn.gov.au/Documents/Australian+Government+s+Critical+Infrastructure+Resilience+Strategy.pdf](http://www.tisn.gov.au/Documents/Australian%2BGovernment%2Bs%2BCritical%2BInfrastructure%2BResilience%2BStrategy.pdf)

Government of Australia, Department of Energy, Resources, and Tourism, *Critical Energy Infrastructure Protection and Resilience,*

<http://www.ret.gov.au/energy/energy_security/critical_infrastructure_protection_and_resilience/Pages/CriticalInfrastructureProtectionandResilience.aspx>

Northern Territory Government*, Framework for the Protection of Northern Territory Critical Infrastructure*, (January 2009),

<http://www.dcm.nt.gov.au/__data/assets/pdf_file/0015/44610/NT_CIP_Framework.pdf>

*American Samoa Tsunami Study Research Topic #03 Critical Infrastructure,* (September 2011),

<http://astsunamiresilience.org/asts/wp-content/uploads/2011/06/3.-Critical-Infrastructure_ASTS-092711_reduced.pdf>

*Journal of Energy Security, Critical Energy Infrastructure Protection: The Case of the Trans-ASEAN Energy Network,* (August 27, 2009),

<http://www.ensec.org/index.php?option=com_content&view=article&id=205:critical-energy-infrastructure-protection-the-case-of-the-trans-asean-energy-network&catid=98:issuecontent0809&Itemid=349>

1. **Additional Recommended Reading:**

 *Critical Infrastructure Protection: Survey of World-Wide Activities,* (2004), <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Kritis/paper_studie_en_pdf.pdf?__blob=publicationFile> (Asia-Pacific countries only)

**lesson 9 topic: managing cyber risks to critical infrastructure: the international landscape part i**

**1. Lesson Goals/Objectives:**

* Discuss the “borderless” nature of the cyber threats and challenges that impact the critical infrastructure security and resilience mission area.
* Examine the international linkages between cybersecurity and critical infrastructure security and resilience, including dependencies, interdependencies, and supply chain implications.
* Identify and discuss the authorities, capacities and resources landscape of the cyber domain as they pertain to the international dimension of critical infrastructure security and resilience.
* Identify and discuss the global challenges presented by information technology and supervisory control and data acquisition (SCADA) system vulnerabilities.
* Explain how cyber risk is assessed and managed internationally within and across the various critical infrastructure sectors, as well as how cyber risk mitigation performance is evaluated.
* Evaluate the different international perspectives on cybersecurity as well as some of the various national and multilateral approaches used to secure the cyber components of critical infrastructure systems.

**2. Discussion Topics:**

* What are the principal threats and challenges associated with cybersecurity as they pertain to international critical infrastructure security and resilience? Is this a “real and present danger?” Why or why not?
* How does the United States approach cybersecurity issues domestically and in the context of international collaboration?
* Discuss the major components of the Executive Order 13636, *Improving Critical Infrastructure Cybersecurity* and the *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World.* What are the strengths and weaknesses of the U.S. approach?
* How is the European Community dealing with the cyber threat to critical infrastructure? Is this an effective approach? Why or why not?
* Who “owns” the cyber problem internationally? On the government side? On the private sector side? How does each party communicate and coordinate with the other to jointly address cyber risk?
* How do various foreign governments view cybersecurity? Is their perspective similar or different from the U.S. perspective? Why or why not?
* What are the risks presented by SCADA systems? How do cyber and SCADA concerns relate to the critical infrastructure sectors internationally? How can the international community best come together to address SCADA-related vulnerabilities?
* How can cyber risk be assessed and mitigated on an international scale? Unilaterally, bilaterally or multilaterally? How do we know when we are making a difference in this domain? How can risk reduction be measured?
* Is regulation required to mitigate risk internationally across all sectors subject to the cyber threat? If so, what might such a regime look like?

**3. Required Reading:**

Peter Allor, *Understanding and Defending Against Foreign Cyber Threats*, (2007),

<http://www.homelandsecurity.org/journal/Default.aspx?oid=165&ocat=1>.

Eugene Nickolov, *Critical Information Infrastructure Protection: Analysis, Evaluation, and Expectations,* (2005), <http://www.comw.org/tct/fulltext/05nickolov.pdf>

Statement of Gregory C. Wilshusen, Testimony Before the Subcommittee on Oversight, Investigations, and Management, Committee on Homeland Security, House of Representatives, *Cybersecurity Threats Impacting the Nation,* (April 24, 2012),

<http://www.gao.gov/assets/600/590367.pdf>

Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, 2013. <http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>.

National Institute of Standards and Technology, *Framework for Improving*

*Critical Infrastructure Cybersecurity*, February 12, 2014, <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf>.

The White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, (May 2011), <http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>.

International Code of Conduct for Information Security, <http://www.rusemb.org.uk/policycontact/49>.

George Davies, *Addressing the Cybersecurity Th*reat, (January 13, 2013),

<http://www.businessrevieweurope.eu/technology/software/addressing-the-cyber-security-threat>

European Commission, *Protecting Europe from Large-scale Cyber attacks and Disruptions: Enhancing Preparedness, Security and Resiliency*, (2009),

<http://ec.europa.eu/information_society/policy/nis/docs/comm_ciip/comm_en.pdf>.

European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions, *On Critical Information Infrastructure Protection: Achievements and Next Steps: Towards Global Cyber-Security*, (March 2011), <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:EN:PDF>.

Adam Segal and Matthew Waxman, *Why a Cybersecurity Treaty is a Pipe Dream,* (October 27, 2011),

<http://globalpublicsquare.blogs.cnn.com/2011/10/27/why-a-cybersecurity-treaty-is-a-pipe-dream/>

Idaho National Laboratory, *Vulnerability Analysis of Energy Delivery Control Systems*, (September 2011),

<http://energy.gov/sites/prod/files/Vulnerability%20Analysis%20of%20Energy%20Delivery%20Control%20Systems.pdf>

USCERT, *Cross Sector Roadmap for Cyber-Security of Control Systems*, (September 30, 2011), <http://www.us-cert.gov/control_systems/pdf/Cross-Sector_Roadmap_9-30.pdf>

Reporting and Analysis Centre for Information Assurance MELANI, <http://www.melani.admin.ch/index.html?lang=en>.

**4. Additional Recommended Reading:**

The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, (2009),

<http://whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf>.

Mariana Hentea, *Improving Security for SCADA Control Systems*, (2008),

<http://ijikm.org/Volume3/IJIKMv3p073-086Hentea361.pdf>.

Stouffer, Falco, and Kent, *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrialized Control Systems Security*,(2006),

[http://www.cyber.st.dhs.gov/docs/NIST%20Guide%20to%20Supervisory%20and%20Data%20Acquisition-SCADA%20and%20Industrial%20Control%20Systems%20Security%20(2007).pdf](http://www.cyber.st.dhs.gov/docs/NIST%20Guide%20to%20Supervisory%20and%20Data%20Acquisition-SCADA%20and%20Industrial%20Control%20Systems%20Security%20%282007%29.pdf).

George Mason University, The Center for Infrastructure Protection and Homeland Security, *The CIP Report*, 7(8), (February 2009), <http://tuscany.gmu.edu/centers/cip/cip.gmu.edu/wp-content/uploads/2013/06/CIPHS_TheCIPReport_February2009_SCADA.pdf>.

George Mason University, The Center for Infrastructure Protection and Homeland Security, *The CIP Report*, 9(7), (January 2011), <http://tuscany.gmu.edu/centers/cip/cip.gmu.edu/wp-content/uploads/2013/06/CIPHS_TheCIPReport_January2011__Cybersecurity.pdf>.

U.S. Government Accountability Office, *Cybersecurity: Continued Attention is Needed to Protect Federal Information Systems from Evolving Threats*,(2010),

<http://www.gao.gov/new.items/d10834t.pdf>.

**lesson 10 topic: managing cyber risks to critical infrastructure: the international landscape part ii**

**\*\*special activity**: **in-class exercise activity**

Today’s class involves an interactive, discussion-based activity in which the class will be organized into small groups to examine various national, bi-national and multinational approaches to international cybersecurity. Group assignments will be made at the end of class on Lesson 9. Each learner group will examine an existing national, bilateral or multilateral approach and present key elements thereof to the class. These elements will include considerations such as 1) authorities; 2) concepts of operations; 3) risk assessment protocols; 4) risk management approaches (voluntary & regulatory); 5) information sharing; and 6) legal regimes. The individual learner groups will provide a critical analysis of these various elements and recommend alternative approaches or strategies as appropriate. This assignment will require additional Internet research. No formal presentation will be required.

**1. Lesson Goals/Objectives:**

* Summarize alternative approaches to the cybersecurity aspects of critical infrastructure security and resilience in use internationally, including voluntary and regulatory models.
* Compare and contrast the efficacy of these various approaches.
* Identify and examine the efficacy of various structures and forums that are used to promote international cybersecurity cooperation and collaboration.

**2. Discussion Topics:**

* How does the United States approach the cybersecurity dimension of critical infrastructure security and resilience?
* What are some of the approaches to cybersecurity used outside the United States? What are their strengths and weaknesses? Is the United States more consistent with some approaches than others? Why or why not?
* How does the international community view the United States approach towards cybersecurity? Does the international community have the same concerns as the United States? Why or why not?
* What are some examples of countries that use a purely voluntary approach to cybersecurity in the context of critical infrastructure security and resilience? A purely regulatory approach? A hybrid approach?
* Is there an appropriate structure(s) through which international cybersecurity issues can be addressed?
* Is there a national, bi-national, or multi-national cybersecurity program that stands out as a model or best practice?
* How can bilateral/multilateral cybersecurity cooperation and collaboration be incentivized?

**3. Required Reading:**

Ross Anderson and Shailendra Fuloria, *Security Economics and Critical National Infrastructure,*

<http://www.cl.cam.ac.uk/~rja14/Papers/econ-cni09.pdf>

Public Safety Canada, *Canada’s Cyber Security Strategy for a Stronger and More prosperous Canada,* (2010),

<http://www.publicsafety.gc.ca/prg/ns/cybr-scrty/ccss-scc-eng.aspx>

Government of Australia, *Cyber Security Strategy*, (2009),

<http://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf>

*GOV.UK Website, The UK Cyber Security Strategy, (Various Documents), (2011-2012),* <https://www.gov.uk/government/publications/cyber-security-strategy>

European Network and Information Security Agency, *Dutch, French, and German Cyber Security Strategies Presented,* (February 25, 2011), <http://www.enisa.europa.eu/media/news-items/cyber-security-strategies-of-de-nl-presented>

Peter Sommer and Ian Brown, Reducing Systemic Cyber Security Risk, (January 14, 2011), [*http://www.oecd.org/governance/risk/46889922.pdf*](http://www.oecd.org/governance/risk/46889922.pdf)

European Network and Information Security Agency, *New EU Cyber Security Strategy and Directive Announced*, (February 7, 2013), [*http://www.enisa.europa.eu/media/news-items/new-eu-cybersecurity-strategy-directive-announced*](http://www.enisa.europa.eu/media/news-items/new-eu-cybersecurity-strategy-directive-announced)

Marcin Terlikowski and Jozef Vyskoc, *Coming to terms with a New Threat: NATO and Cyber-Security,* (February 7, 2013), [*http://www.cepolicy.org/publications/coming-terms-new-threat-nato-and-cyber-security*](http://www.cepolicy.org/publications/coming-terms-new-threat-nato-and-cyber-security)

APEC Cyber Security Strategy,

[*http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan012298.pdf*](http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan012298.pdf)

Office of the Auditor General of Canada, *2012 Fall Report of the Auditor General of Canada, Chapter 3 – Protecting Canadian Critical Infrastructure Against Cyber Threats*, (2012)

[*http://www.oag-bvg.gc.ca/internet/English/parl\_oag\_201210\_03\_e\_37347.html*](http://www.oag-bvg.gc.ca/internet/English/parl_oag_201210_03_e_37347.html)

*Additional Internet research as required to support group discussion assignments.*

1. **Additional Recommended Readings**

<http://www.infosecisland.com/blogview/4291-DHS-Cyber-Security-Resources-Catalog.html> (DHS Cyber Resources Catalog)

Government Accountability Office, *Cybersecurity Guidance is Available, but More Could be Done to Promote its Use*, (2011), <http://www.gao.gov/products/GAO-12-92>

<http://www.nerc.com/page.php?cid=2%7C20> (Cybersecurity regulatory standards)

**lesson 11 topic: global infrastructure interdependencies and supply chain security: part i**

**1. Lesson Goals/Objectives**:

* Explain and provide examples of how dependencies, interdependencies, and supply chain issues impact critical infrastructure risk assessment and management on a global scale.
* Discuss how critical infrastructure sectors such as energy, transportation, and communications approach dependencies/interdependencies, including cross-sector cybersecurity risk and supply chain risk.
* Provide examples of how infrastructure and supply chain considerations are factored into the international public-private sector planning process, as well as gaps in this process.
* Discuss how dependencies/interdependency and supply chain related issues produce borderless consequences and complicate incident response decision making and infrastructure restoration operations.
* Identify and discuss the major elements of a successful global supply chain strategy.

**2. Discussion Topics**:

* What approaches are used by governments and private industry to address critical infrastructure dependencies and interdependencies across national borders and boundaries?
* How do dependencies, interdependencies, and supply chain issues relate to critical infrastructure risk at the international level?
* How can dependencies/interdependencies best be accounted for in the planning process within and across the critical sectors and international borders?
* What kinds of borderless impacts do international infrastructure dependencies/interdependencies typically produce in the context of manmade and naturally occurring disasters? How do these dependencies/interdependencies complicate incident response decision making and infrastructure restoration and recovery operations?
* What types of risk are represented by the “geographic clustering” of critical infrastructure on an international basis? How has this risk manifested itself in recent real world natural disaster situations?
* How do international supply chains complicate traditional approaches to risk assessment and management?
* What are the major goals and guiding principles that underpin the United States National Strategy for Global Supply Chain Security? How does this strategy address critical infrastructure dependencies/ interdependencies issues? How does the Strategy propose to reduce critical offshore infrastructure vulnerabilities beyond the control of the United States?
* How can a global strategy addressing supply chain security best be implemented, and is there an appropriate mechanism(s) through which implementation could be accomplished and/or incentivized?
* How do we achieve critical infrastructure security and resilience in the context of a global economy?

**3. In-Class Exercise**: Learners should be prepared to discuss critical infrastructure dependencies/interdependencies in the context of recent international incidents such as the Japanese Tsunami, Iceland Volcano, Gulf Coast Oil Disaster, North American Power Blackout, etc.). The focus of the discussion will be on international impacts and risk response activities, along with key lessons learned. Learner real world incident assignments will be made at the end of class on Lesson 10. This assignment will require additional Internet research. No formal presentation will be required.

**4. Required Reading**:

Steven Rinaldi, James Peerenboom, and Terrence Kelly, *Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies*, (2004), <http://www.ce.cmu.edu/~hsm/im2004/readings/CII-Rinaldi.pdf>.

George Mason University, The Center for Infrastructure Protection and Homeland Security (CIP/HS), *The CIP Report*, 10(2), (August 2011), <http://tuscany.gmu.edu/centers/cip/cip.gmu.edu/wp-content/uploads/2013/06/CIPHS_TheCIPReport_August2011_Interdependencies.pdf>.

George Mason University, The Center for Infrastructure Protection and Homeland Security (CIP/HS), *The CIP Report*, 10(1), (July 2011),

<http://tuscany.gmu.edu/centers/cip/cip.gmu.edu/wp-content/uploads/2013/06/CIPHS_TheCIPReport_July2011_GlobalSupplyChain.pdf>.

Michel Van Eeten, Albert Nieuwenhuijs, Eric Luiijf, Marieke Klaver, and Edite Cruz, “The State and the Threat of Cascading Failure across Critical Infrastructures: The Implications of Empirical Evidence from Media Incident Reports,” *Public Administration*, 89(2), (2011), 381–400, <http://onlinelibrary.wiley.com/doi/10.1111/j.1467-9299.2011.01926.x/abstract>

Congressional Research Service Report*, Vulnerability of Concentrated Critical Infrastructure: Background and Policy Options*, (2006),

<http://assets.opencrs.com/rpts/RL33206_20080912.pdf>.

T.D. O’Rourke, *Critical Infrastructures, Interdependencies, and Resilience*, (Spring 2007), <http://www.nae.edu/Publications/Bridge/EngineeringfortheThreatofNaturalDisasters/CriticalInfrastructureInterdependenciesandResilience.aspx>

National Defense University, *Strategic Fragility: Infrastructure Protection and National Security in the Information Age*, (2008), <http://www.carlisle.army.mil/DIME/documents/Miller%20and%20Lachow%20Strategic%20Fragility.pdf>.

The Infrastructure Security Partnership, *The Infrastructure Security Partnership, Infrastructure Resilience, and Interdependencies*, (March 2010), <http://www.tisp.org/index.cfm?cdid=11972&pid=10261>.

Dave Thomas, Trey Hanbury, Ray Rutngamlug, and A.J. Burton. *Super Storm Sandy Foreshadows a New Paradigm of Protecting Critical Communications and Electric Infrastructure*, (2012),

<http://www.hlregulation.com/2012/11/12/superstorm-sandy-foreshadows-a-new-paradigm-for-protecting-critical-communications-and-electric-infrastructure/>

The White House, *National Strategy for Global Supply Chain Security*, (January 2012), <http://www.whitehouse.gov/sites/default/files/national_strategy_for_global_supply_chain_security.pdf>

International Atomic Energy Agency, *Report of Japanese Government to IAEA Ministerial Conference on Nuclear Safety-Accident at TEPCO’d Fukushima Nuclear Power Stations*,(June 7, 2011), <http://www.iaea.org/newscenter/focus/fukushima/japan-report/>.

1. **Additional Recommended Reading:**

National Infrastructure Advisory Council,

*Framework for Dealing with Disasters and Related Interdependencies*, (July 2009), <http://www.dhs.gov/xlibrary/assets/niac/niac_framework_dealingwithdisasters_slides.pdf>

Xavier Guiho, Patrick Lagadec, and Erwan Lagadec,

*Non-conventional Crises and Critical Infrastructure: Katrina*, (2006), <http://www.patricklagadec.net/fr/pdf/EDF-Katrina-Report-31.pdf>.

**lesson 12 topic: global infrastructure interdependencies and supply chain security: part ii**

**\*\*special activity**: **in-class exercise activity**

Today’s class involves an interactive, discussion-based activity in which the class will be organized into small groups to examine various national, bi-national and multinational approaches to global supply chain security. Group assignments will be made at the end of class on Lesson 11. Each learner group will examine an existing approach and present key elements thereof to the class. These elements will include considerations such as 1) authorities; 2) concepts of operations; 3) risk assessment protocols; 4) risk management approaches (voluntary & regulatory); 5) information sharing; and 6) legal regimes. The individual learner groups will provide a critical analysis of these various elements and recommend alternative approaches or strategies as appropriate. This assignment will require additional Internet research. No formal presentation will be required.

**1. Lesson Goals/Objectives:**

* Assess the complex global security and economic environments in which the U.S. and other nations must interact, including the various threats and hazards that challenge supply chain security from a public-private perspective.
* Identify and discuss the major elements of a successful global supply chain strategy.
* Compare and contrast various national, bi-national, and multinational approaches to global supply chain security.
* Articulate the major goals and guiding principles that underpin various approaches to global supply chain security.
* Explain how global supply chain security strategies account for risks and interdependency factors that extend beyond the borders of any single nation.
* Provide examples of how supply chain considerations are factored into the international public-private sector planning process, as well as gaps in this process.

**2. Discussion Topics:**

* Discuss the wide array of threats and hazards that can potentially impact supply chain security.
* What are the major elements of a successful global supply chain security strategy? How does these elements relate to one another?
* What are the major obstacles/impediments to global supply chain security?
* What are the major goals and guiding principles that underpin the various national and international various approaches to global supply chain security? How do these approaches address critical infrastructure dependencies/ interdependencies issues and offshore infrastructure vulnerabilities beyond the control of any single nation?
* Is there any particular approach that seems more effective than the others? If so, why? What role should regulation play?
* How can a global strategy addressing supply chain security best be implemented, and is there an appropriate mechanism(s) through which implementation could be accomplished and/or incentivized?
* How do we achieve supply chain security in the context of a global economy?

**3. Required Reading:**

APEC Website, *APEC Adopts Strategy for Securing Commerce in the Asia-Pacific Region*, (Various Documents)

<http://www.apec.org/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Task-Groups/Counter-Terrorism-Task-Force/Secure-Trade-Factsheet.aspx>

Henry H. Willis and Davis S. Ortiz, *Evaluating the Security of the Global Containerized Supply Chain,* (2004), (February 7, 2012), <http://www.trb.org/MarineTransportation1/Blurbs/155274.aspx>

Statement of Stephen L. Caldwell, Testimony Before the Subcommittee on Maritime and Border Security, Committee on Homeland Security, U.S. House of Representatives, *Container Security Programs Have Matured, But Uncertainty Persists over the Future of 100 Percent Scanning*, <http://www.gao.gov/assets/590/588253.pdf>

Cross-Border Research Association, *Critical Infrastructure and Supply Chain Protection*, (January 2012) <http://www.focusproject.eu/documents/14976/014b8126-d528-4b01-a73a-e56ecce70f74>

Additional Internet research as required to support learner group discussions.

**lessons 13 & 14 topic: learner research presentations**

**\*\*special activity: final research papers are due via e-mail prior to class on lesson 14.**

**1. Lesson Goals/Objectives:**

* Present an examination of an international critical infrastructure security and resilience issue or a critique of a national (non-United States), bi-national, or multinational critical infrastructure security and resilience-related policy, strategy or plan.

**2. Discussion Topics:**

* Learner presentations.

**3. Required Reading:**

* As required for individual research paper development and presentation.

**lesson 15 topic: preparing for the international risk environment of the future and course critique**

**1. Lesson Goals/Objectives:**

* Apply concepts learned throughout the course to evaluate the future challenges and the evolving operational environment for international critical infrastructure.
* Apply knowledge and concepts of this course to evaluate the implications of issues such as global climate change, aging populations, decaying infrastructures, dependencies and interdependencies, and ever more consequential natural disasters on international critical infrastructure security and resilience.
* Assess strategic choices that may impact our approach to international critical infrastructure security and resilience and supply chain security in the medium-long term future (10-20 years from now).
* Identify and discuss the types of investments that must begin to happen now—on a national, bi-national, and multinational basis—to adequately prepare for the future world of international critical infrastructure security and resilience.

**2. Discussion Topics:**

* What will the international critical infrastructure security and resilience operational environment look like 10-20 years from now? How might it differ from the environment we face today?
* How will the continuing evolution of information and communications technology and transportation systems impact this future operating environment?
* What will be the principal threats and challenges to international critical infrastructure security and resilience and supply chain security in this future world?
* How will malicious actor threats impact the future critical infrastructure security and resilience environment internationally?
* How will issues like global climate change, aging populations, decaying infrastructures, solar weather and ever more consequential natural disasters impact international critical infrastructure security and resilience in the future?
* What insights do we have on the nature of future critical infrastructure dependencies and interdependencies on an international scale?
* How might we best approach the issues of international partnerships and information sharing in this future world?
* What actions should the international community be taking or what investments should it be making now to buy down future risk and position the next generation for success in this mission area? Will today’s priorities set us up for success or will they fall short in some important way?
* How might future critical infrastructure security and resilience and supply chain security requirements best be determined and resourced on a global scale?
* How do we begin to address international concerns that transcend the next budget cycle or that require extensive bi-national or multinational cooperation and collaboration?
* How can we achieve truly integrated international government-private critical infrastructure security and resilience planning in the future? How can critical infrastructure security and resilience goals and objectives be harmonized across national boundaries?

Course Critique:

* What are your overall thoughts on this course and the instructional methodology used? The course research project/oral presentation? In-class exercise activities?
* What are your thoughts on the reading materials assigned and the amount of reading assigned per lesson? Were any readings more helpful than others?
* How can the course be improved? Do you have any suggestions regarding additional in-class student activities?

**3. Required Reading:**

Toffler Associates, *Guarding Our Future: Protecting our Nation’s Infrastructure*, (2008), <http://www.toffler.com/docs/Guarding-Our-Future.pdf>.

Toffler Associates, *Five Critical Threats to the Infrastructure of the Future*, (2008), <http://www.toffler.com/docs/Five-Critical-Infrastructure-Threats.pdf>.

Sandra I. Erwin, Stew Magnuson, Dan parsons, and Yasmin Tadjdeh, *Top Five Threats to National Security in the Coming Decade,*(November 2012),

<http://www.nationaldefensemagazine.org/archive/2012/November/Pages/TopFiveThreatstoNationalSecurityintheComingDecade.aspx>

Instituto Nacional de Tecnico Aerospacial, *Alternative Futures of Security Research for Critical Infrastructure & Supply Chain Protection,* (2012)

<http://www.focusproject.eu/documents/14976/c87be56d-fcbc-4a36-9b4e-58b4e4925e4d>

James Neumann, *Adaptation to Climate Change: Revisiting Infrastructure Norms,* (December 2009),

<http://www.rff.org/RFF/Documents/RFF-IB-09-15.pdf>

Nikolai Bobylev, *Urban Underground Infrastructure and Climate Change: Opportunities and Threats,* (2*0*009),

<http://siteresources.worldbank.org/INTURBANDEVELOPMENT/Resources/336387-1256566800920/6505269-1268260567624/Bobylev.pdf>

Henry G. Schwartz, Jr., *Adaptation to the Impacts of Climate Change on Transportation,* (Fall 2010),

<http://www.nae.edu/Publications/Bridge/24514/24525.aspx>

Continuity Central, *Critical Infrastructure: Time to Begin Anticipating and Adapting to Climate Change,*

<http://www.continuitycentral.com/news05883.html>

Tom Ridge and Robert B. Stephan, *Preparing for 21st Century Risks: Revitalizing American Manufacturing to Protect, Respond and Recover*, (July 2012), <http://americanmanufacturing.org/homeland>

Brian Vastag, “As the Sun Awakens, the Power Grid Stands Vulnerable,”

*Washington Post*, (June 20, 2011), <http://www.washingtonpost.com/national/science/as-the-sun-awakens-the-power-grid-stands-vulnerable/2011/06/09/AGwc8DdH_story.html?hpid=z2>.

North American Electric Reliability Corporation, *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System,* (June 2010),

<http://www.nerc.com/files/HILF.pdf> (Executive Summary only)

European Union, *“Security as Social Science” – Critical Infrastructure and Supply Chain Research Driven by Society,* (2010),

[http://www.focusproject.eu/web/focus/wiki/-/wiki/REFERENCE\_SCENARIOS/%E2%80%9CSecurity+as+Societal+Science%E2%80%9D+-+Critical+infrastructure+and+supply+chain+research+driven+by+societal+factors](http://www.focusproject.eu/web/focus/wiki/-/wiki/REFERENCE_SCENARIOS/%E2%80%9CSecurity%2Bas%2BSocietal%2BScience%E2%80%9D%2B-%2BCritical%2Binfrastructure%2Band%2Bsupply%2Bchain%2Bresearch%2Bdriven%2Bby%2Bsocietal%2Bfactors)

Federal Emergency Management Agency, *Crisis Response and Disaster Resilience 2030: Forging Strategic Action in the Age of Uncertainty,* (January 2012),

<https://www.fema.gov/library/file;jsessionid=8554589B27DB7D4F10DB35D4956ED5BB.Worker2Library?type=publishedFile&file=sfi_report_13.jan.2012_final.docx.pdf&fileid=70ed3250-4114-11e1-8c9e-001cc456982e>