

Department of Security Studies

Syllabus

Critical Infrastructure Protection (face to face)

SCST 5348

Spring 2018

Security Studies Department

College of Criminal Justice

Sam Houston State University

Instructor: Assistant Professor Russell Lundberg

Class hours: Thursdays, 3-5:50

Office: TBA

Office Hours: Thursdays, 2-3

Classroom: TWC 235

Office Phone: (936) 294-3634

Skype: Russell.lundberg

Email: russell.lundberg@shsu.edu

Course Description

Our society is increasingly reliant on technologies to make our everyday activities possible. Everything from the food we eat and water we drink to the transfer of information and energy are made possible from systems that lie under the surface of modern life. These systems make our lives easier and more capable, but we become reliant on them for everyday functions, and we need to understand the interdependencies and the difficulties of governing sprawling infrastructures across many sectors. Nothing could be more important than the protection of infrastructure so critical that it has become the foundation of our civilization.

Course Textbook

1. Lewis, Ted G. (2014) *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*. John Wiley & Sons. [Lewis]

Additional readings will be made available online, including but not limited to journal articles, government reports, and critical infrastructure association web pages and resources.

Course Skill Development Goals

Essential Goals

1. "Learning to apply course material (to improve thinking, problem solving and decisions)" to critical Infrastructure protection activities in the homeland security enterprise.
2. "Developing specific skills, competencies, and points of view needed by professionals in the field most closely related to" critical infrastructure protection as part of the homeland security enterprise.

Important Goals:

1. “Acquiring skills in working with others as a member of a team” by participating in online discussions with classmates, and presenting to instructor and classmates.
2. “Learning to analyze and critically evaluate ideas, arguments, and points of view” by participating in online discussions on course readings and the course research paper assignment.
3. “Developing skill in expressing oneself orally and in writing.” It is important to be able to communicate the concepts of critical infrastructure to practitioners, skills that we will develop through written memos.

Substantive Course Goals

The substantive goals of this course are to familiarize students with the theoretical foundations of critical infrastructure protection using seminal works in the field such as Ted Lewis’s *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation* and teach students to apply these concepts to real world infrastructures. Ultimately the goal of this course is to improve the security of the United States and world by coming to deeper understandings of critical infrastructure governance and interdependencies through the creation of a cadre of professionals with a deeper understanding of these issues and theoretical frameworks. Students will become familiar with the principles of Ted Lewis’s work on model based vulnerability analysis (MBVA). This course will provide students with tangible certifications in the field of critical infrastructure protection through the utilization of FEMA online training courses and is part of a larger certification in critical infrastructure from Sam Houston State University which is in turn part of a larger Master program in Homeland Security in the Security Studies Department.

Office Hours

The professor will be available one hour before class every week in an office to be arranged. Additionally, the professor will attempt to be available for reasonable requests for synchronous meetings (either Skype or other media) and will attempt to respond to any emails within 24 hours. Professors get into teaching because they are interested in having their students succeed, and I encourage you to reach out to me with any questions, comments, or interesting ideas that you have during the course of the class.

Academic Honesty Policies

Students will be held to the highest standards of academic honesty. Students should review the academic honesty policies of Sam Houston State University available here http://www.shsu.edu/dept/academic-affairs/faculty-handbook/academic_dishonesty.html and should expect enforcement in accordance with the highest standards of those policies. Academic dishonesty includes not only direct copying of the text of others but many ways of excessively relying on the thoughts of others without adding thought of your own; see http://turnitin.com/assets/en_us/media/plagiarism_spectrum.php for different types of academic dishonesty. The instructor reserves the right to check papers against a national anti-plagiarism database. Academic dishonesty can result in punishment ranging from failing the assignment to failing the class to expulsion from the program.

Opportunity for Course Feedback at Mid-point

The instructor will provide regular feedback to students via discussion boards, email, and office hours. The instructor also welcomes and appreciates feedback on the course design. Given this is the inaugural

class in a new program, student feedback will be critical to the improvement of future iterations of the course. Students should feel free to email the instructor on any issue they think could be improved.

Religious Holidays

Accommodations will be made to students for religious holidays and the associated travel needed for them in accordance with Texas state law and the policies of Sam Houston State University. If students have any questions or concerns they should not hesitate to contact the instructor via email.

Disabilities

Any student seeking reasonable accommodation for a disability in accordance with federal, state, local law and policy of Sam Houston State University must contact Offices of Students with Disabilities located in the Counseling Center. <http://www.shsu.edu/dept/disability/>
After contacting this office students should feel free and comfortable contacting the instructor about any disability issue so that reasonable accommodations can be made.

Course Assignments

1. Participation in weekly discussions (39%)
2. Research Paper Proposal (1 page) (3%)
3. Research Paper Draft (8-10 page) (10%)
4. Research Paper Final (15-20 page) (25%)
5. 1 Group Exercise (5%)
6. 6 FEMA Online Training Courses and Certifications (18%)

Weekly Discussions:

Each week students will respond in to prompts from the instructor based on the themes, readings, brief online lectures, and assignments of that week. Students should be present and engaged. This does not mean that students need to participate every week—quality of contribution is more important than quantity—but they should be ready to participate when asked with discussions that are well considered and in depth. Students should not simply answer questions with short answers but explain their answers in an extended form. Students should reference that material where appropriate as well as outside sources or examples. They should think about the materials critically and should feel free to ask questions and take the discussion in various directions. Discussion should be more than simple agreement or appreciation for the comments of others; whether you agree or disagree, you should move the conversation forward in engaging with these issues.

In addition to participating in discussions every week, each student will have the responsibility to lead the discussion in one week. Weeks will be assigned for each student by the professor at the outset of class although students may trade for other weeks if they so choose. The students should, at the very least, identify the most important points in the readings and be prepared with prompts for students to engage the material more deeply. This may take the form of a specific example, a thought exercise, an additional perspective, or other approach.

It is important for the discussions to be both critical and respectful. It is important that students are respectful in communications with each other. While students can and should engage with each other's ideas, probing and contradicting where appropriate, students should still communicate in a professional and collegial matter.

Research Paper (38 points combined including draft and proposal)

Given this will be the first research writing assignment in the Critical Infrastructure certificate program, the course is designed to help students succeed. Students will turn in a 1 page double spaced 12 point font topic proposal on a critical infrastructure topic of their choice for approval from the instructor in week 4. This will allow the instructor to give feedback on the topic chosen, the quality of the idea and the feasibility of the project. The topic paper will largely be graded on pass/fail basis provided it is of sufficient quality and effort. The proposal must be cited in proper APA format. The instructor strongly recommends the use of citation management software such as Endnote (paid software) or Zotero (free online at Zotero.org). All papers should be turned in in MS Word so that the instructor can provide feedback via track changes.

In week 9 students will turn in an 8-10 page double-spaced draft of their paper incorporating the feedback of the instructor from the proposal. This will allow the instructor to gauge student progress and provide another round of useful feedback to maximize the quality of the final research paper. Paper drafts will be graded on the quality of writing, substantive ideas, and research conducted. All of the papers must be properly cited in APA format.

The final research paper assignment is due in class on May 3th. It must be 15-20 pages double spaced with 12 point times new roman font with a full bibliography and properly cited in APA format. Research papers will be graded on the quality of writing, substantive ideas, research conducted, and how well they incorporated instructor feedback.

1 Exercises (5 points each)

There will be one exercise in a week in which no discussion boards are planned. Details on the exercises will be forthcoming. Students will get their assignment in the week before and will need to coordinate with the class on a time to participate in the activity. Students will be graded based upon the quality of their participation.

6 FEMA Online Training Certifications (3 points each)

The course includes 6 FEMA online training courses and certificates on relevant topics. Links will be provided to the courses in the weekly schedule. Students must complete these individually. Cheating on these exams may be reported by FEMA to the Instructor and will result in academic sanction. Students must submit evidence of completion to the instructor via email or in the assignment upload link in the weekly schedule in blackboard. Students are strongly encouraged to upload these certificates of completion to their Preparingtexas.org resume. Must be completed Sunday (midnight) at the end of the week assigned. These training certifications will be graded on a pass/fail basis. Unexcused late submissions will be subject to reduced points.

Class Hours

The class is presented on a standard weekly schedule, with one week of readings, lectures, and assignments per week.

Weekly Schedule

	Date	Subject	Readings	Assignments
0	1/18	Intro to Class	1. No readings, but online videos	Discussion:

				Introduce yourself (no points)
1	1/25	Intro to CI	<ol style="list-style-type: none"> 1. Lewis, Ch. 1 2. I, Pencil (video) 3. American Society of Engineers, “2013 Report Card for America’s Infrastructure,” http://infrastructurereportcard.org/a/#p/overview/executive-summary 	Discussion: Describe an Infrastructure
2	2/1	Challenges in CI	<ol style="list-style-type: none"> 1. Auerswald, Philip, Lewis M. Branscomb, Todd M. La Porte, and Erwann Michel-Kerjan. “The Challenge of Protecting Critical Infrastructure.” Wharton University of Pennsylvania: Risk Management and Decision Processing Center, 2005. (14 pages) available at http://issues.org/22-1/auerswald/ 2. Critical Infrastructure Protection and the Private Sector: The Crucial Role of Incentives. Peter Orszag. Brookings Institution. 2003. 3. Bellavita (2011) “How Proverbs Damage Homeland Security” Homeland Security Affairs https://www.hsaj.org/articles/62 	Discussion: Describe an Ownership IS-913a CISR: Achieving Results through Partnership and Collaboration
3	2/8	Risk Strategies	<ol style="list-style-type: none"> 1. Lewis 2 	Discussion: Threats to CI IS-906 Workplace Awareness
4	2/15	Theories of Catastrophe	<ol style="list-style-type: none"> 1. Lewis 3 	Discuss Research Paper Proposal
5	2/22	Networks	<ol style="list-style-type: none"> 1. Lewis 4 2. Barabasi, A.L., and E. Bonabeau (2003) “Scale-Free Networks” Scientific American, May 2003. http://www.barabasilab.com/pubs/CCNR-ALB_Publications/200305-01_SciAmer-ScaleFree/200305-01_SciAmer-ScaleFree.pdf 3. Newman, M.E.J. (2003) “The Structure and Function of Complex Networks” arXiv. http://math.uchicago.edu/~shmuel/Network-course-readings/Newman,%20SIAM.pdf [Read pages 1-20; additional pages optional] 	Discussion: Describe a Network
6	3/1	Risk Management	<ol style="list-style-type: none"> 1. NIPP 2013 Partnering for Critical Infrastructure Security and Resilience. 	Discussion

			<p>Department of Homeland Security, 2013.</p> <p>2. <i>The CIP Report</i>. Available at http://cip.gmu.edu/past-issues-catalog/</p> <ul style="list-style-type: none"> a. September 2014 Issue on Risk and Management b. November 2011 Issue on Risk Management c. At least one other issue that interests you 	IS-860.c The NIPP, An Introduction
7	3/8	Protection and Resilience	<ol style="list-style-type: none"> 1. Lord Jopling. "Protecting Critical Infrastructures: What, Why and How?," 2007. http://www.nato-pa.int/default.asp?SHORTCUT=1165 (particularly items 25-53) 2. The White House (2003) "The Physical Protection of Critical Infrastructure and Key Assets" https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf 3. Hart, S. (2015) "Principles of Infrastructure Resilience" CIP Report, January 2015. Center for Critical Infrastructure Protection and Homeland Security, George Mason University. http://cip.gmu.edu/wp-content/uploads/2013/06/The-CIP-Report_January-2015_Resilience.pdf 4. Kahan, J.H. (2015) "Resilience Redux: Buzzword or Basis for Homeland Security" Homeland Security Affairs https://www.hsaj.org/articles/1308 	<p>Discussion</p> <p>IS-921a Implementing CISR</p>
8	3/22	Information Sharing and Response	<ol style="list-style-type: none"> 1. Eileen R., Lawrence. "Federal Efforts Are Helping to Address Some Challenges Faced by State and Local Fusion Centers." Testimony before the Ad Hoc Subcommittee on State, Local, and Private Sector Preparedness and Integration, Committee on Homeland Security and Governmental Affairs, U.S. Senate, April 17, 2008. 2. <i>The CIP Report</i>. Available at http://cip.gmu.edu/past-issues-catalog/ <ul style="list-style-type: none"> o April 2013 Issue on Information Sharing and Partnerships 3. ESF #8 Critical Infrastructure and Key Resources Support Annex available at https://www.fema.gov/pdf/emergency/nrf/nrf-support-cikr.pdf 	<p>Risk Exercise</p> <p>IS-821.a Critical Infrastructure Support Annex</p>

			4. Risk Exercise Materials	
9	3/29	Information Infrastructure	<ol style="list-style-type: none"> 1. Lewis 5, 6, & 10 2. Cyber Attacks Have Already Targeted Critical Infrastructure Around The World And The U.S. Could Be Next available at http://www.cyberwar.news/2015-10-09-cyber-attacks-have-already-targeted-critical-infrastructure-around-the-world-and-the-u-s-could-be-next.html 3. Cybersquirrel1 http://cybersquirrel1.com/ 	<p>Discussion</p> <p>IS-523 Resilient Accord – Exercising Continuity Plans for Cyber Incidents</p> <p>Research Paper Draft</p>
10	4/5	Water	1. Lewis 11	Discussion
11	4/12	Energy	1. Lewis 12 & 13	Discussion
12	4/19	Health and Public Health	1. Lewis 14	Discussion
13	4/26	Transportation and Supply Chains	1. Lewis 15 & 16	Discussion
14	5/3	Emerging Issues	<ol style="list-style-type: none"> 1. DHS (2016) “U.S. Critical Infrastructure 2025: A Strategic Risk Assessment” https://info.publicintelligence.net/DHS-OCIA-CriticalInfrastructure2025.pdf 2. Willis, Henry H., et al. "Current and Future Exposure of Infrastructure in the United States to Natural Hazards." (2016). Available at http://www.rand.org/pubs/research_reports/RR1453.html 3. <i>Executive Summary Risky Business</i>. Accessed July 10, 2014. http://riskybusiness.org/report/national/ (also explore the links) 	<p>Discussion</p> <p>Final Research Paper DUE in class 5/3!!!</p>