HSEM 415: Cyber Domain in the 21st Century
3 Credits
Class Location: Online
Class Meeting Time: TBD
Prerequisites: HSEM 301 or permission of instructor

Instructor Information

Instructor:	O. Shawn Cupp, Ph.D.
Office Hours:	By appointment; hours and days of email availability to be published
Office Location:	TBD
Work Telephone:	TBD
E-mail:	**oscupp@alaska.edu** alternate scupp@kc.rr.com

Class Textbooks/Materials

Harris, Shane, (2014). @War: The Rise of the Military Internet Complex, Houghton Mifflin Harcourt Publishing: New York. ISBN 978-0-544-25179-3 (Required)

Nye, Joseph S. Jr. (2011). The Future of Power. PublicAffairs: New York. ISBN 978-1-61039-069-9 (Required)

Cyber Strategy of the United States 2015, online: http://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy

Covertino Sebastian M., LtCol, DeMattei, Lou Anne, and Knierim, Tammy M. LtCol. (2007). Flying and Fighting in Cyberspace, The Maxwell Papers, Air War College, Maxwell Paper No. 40. (provided on Blackboard)

Langø, Hans-Inge. (2013). Slaying Cyber Dragons: Competing Academic Approaches to Cyber Security. Norsk Utenerikspolitisk Institutt. Norwegian Institute of International Affairs, NUPI Working Paper 820. http://brage.bibsys.no/xmlui/handle/11250/277537

Paul, Richard and Elder Linda. (2006). The Miniature Guide to Critical Thinking and Tools. www.criticalthinking.org/files/Concepts_Tools.pdf

Students expected to stay on top of current events and debates by reading national and international news via reputable sources on the Internet.

**Additional Readings:* Case studies / handouts as assigned. Be prepared to discuss the readings during the week assigned. Readings and links to readings will be available on Blackboard.

Course Description

This course will provide a theoretical and practical overview of cyber as an operating domain, cyber security as a protective requirement, and cyber power as a means to use cyber assets in conflict. This course is designed to teach undergraduate students the history of the cyber domain, practical application of the principles of cyber domain, and understand the context in which the cyber domain could influence current and future conflicts. The course addresses a range of topics to provide the student a solid overall theoretical foundation of cyber as a domain, a source of national security interest, and exposure to the characteristics of cyber commons. The course will provide analysis of case studies, readings, and strategy to enhance understanding of cyber security, cyber power, and the cyber enterprise.

Course Goals

Students in this will learn, analyze, and apply knowledge obtained to the cyber enterprise. The students exposed to historical, theoretical, and application characteristics of the cyber domain. The national security, legal, and commercial aspects are applied to the understanding students attain in the course. This is a foundation course and provides a basic and fundamental understanding of the cyber domain its place in the 21st century.

Student Learning Outcomes

Students will be able to:

- Assess the role of strategy and policy in determining the role of cyber domain application.
- Identify and contrast the theory and application of cyber domain concepts.
- Appraise interrelationships within the cyber domain including strategy, conflict, commerce, legal, and threat aspects.
- Differentiate the legal constraints and regulatory guidance pertaining to the cyber domain including the interagency complexities.
- Propose and support change, or enhancements to the current HSEM planning, coordination and execution effort.
- Assess the importance and future roles of the cyber commons.
- Evaluate the trends and patterns that will determine the future state of the cyber domain.

Instructional Methods

This class will be taught as a hybrid course. A hybrid course uses various delivery methods to best meet course and session outcomes. The blend may consist of any combination of face-to-face classroom instruction, asynchronous discussion forums, and synchronous sessions. Instructional methodologies, including lectures, case studies, small group activities, student presentations and open and directed discussions, are used to actively involve each student in the learning process. When possible and practical, learning activities will be processed to include not only “what” was learned, but the “so what” and “now what” in order to complete the learning cycle. This course requires a computer with internet access, as we will be utilizing Blackboard. Additionally, students will need internet access for assigned discussions involving online research, as well as access to their UA email accounts and a PowerPoint viewer.

Course Policies

Students expected to remain up to date with the scheduled lesson plans on a weekly basis. Students will be penalized for the late submission of class assignments or if they fall behind by more than two weeks (outside of emergency or mutually agreed upon circumstances). Each late assignment will be docked 10% for every day it is late, up to 100%.

Students expected to observe academic honesty. Dishonest practices including giving or receiving assistance in any manner or form during an examination, unauthorized possession of exam questions, and plagiarism (willfully presenting another person's writings, opinions or thoughts as one's own, without proper credit and documentation) will not be tolerated. Violations of the UAF Student Code of Conduct referred to the appropriate authority for possible disciplinary actions including removal of violator from this course.

Evaluation

40% *Research Paper Outline and Term Paper Draft (400 points):* Each student will choose an appropriate topic *(25 points)* prepare and submit an outline of their term paper *(50 points),* submit a draft of their term paper *(125 points),* and turn in the final paper *(200 points).*

Requirements for research paper:

Handout will provide all rubrics for topic, outline, draft, and final research paper submissions.

20% *Critical Analysis (200 points):* There will be two case studies assigned with required analysis to be provided by the student (100 points each). Analysis based upon the intellectual standards outlined within the Paul, Richard and Elder Linda. (2006). *The Miniature Guide to Critical Thinking and Tools* on pages 5-6.

> ***Requirements for Critical Analysis:***
>
> ***Use the Paul and Elder Miniature Guide and conduct analysis with at least four of the identified Elements of Thought and four of the Universal Intellectual Standards. Total page count will vary based upon the analysis conducted but should exceed 6 pages for each case study critical analysis submitted. Instructor will provide case study suggestions for student decision and use.***

20% *Participation (200 points):* Each student is expected to attend class and participate in the classroom debates. If you have more than 3 unexcused absences throughout the semester you will lose 10% of your final grade. Unexcused absences are missing in-person class meeting, failing to participate in class discussions weekly, or failing to log in weekly and turn in assignments on time for online students.

20% *Structured Reflective Journal Comments (200 points):* Providing answers and reflection on a structured basis with four different topics (50 points each). Students will provide their comments and reflections on assigned topics throughout the course. They will occur approximately one every four weeks. We will use the Paul and Elder Miniature Book for conducting these journal entries www.criticalthinking.org/files/Concepts_Tools.pdf .

Requirements for Structured Reflective Journal Comments:

Instructor will provide shell where student will fill in comments. Use of the Elements of Though and Universal Intellectual Standards form the Paul and Elder Miniature guide is highly encouraged.

Course Rubric based upon assignments and grade calculation

Research Paper	400 points
Critical Analysis	200 points
Participation	200 points
Structured Reflective Journal	200 points
Total	**1000 points**

A =	90-100% (900-1000 points)
B =	80-89% (800-899 points)
C =	70-79% (700-799 points)
D =	60-69% (600-699 points)
F =	59 % or less (599 points or less)

Assignment Evaluation Criteria

- Uses complete sentences
- Uses proper grammar
- Response reflect depth of thought and critical thinking skills using Paul and Elder Miniature Guide, p. 5-6, Elements of Thought and Universal Intellectual Standards www.criticalthinking.org/files/Concepts_Tools.pdf
- Provides coherent and reasonable response to all questions
- Integrates real world examples into responses
- Meets submission timeline

Support Services

Students are encouraged to utilize the UAF Writing Center in 801 Gruening (Phone # 474-5314) as needed to assist in the development and refinement of their written products. Students are also encouraged to use the UAF Speaking Center for coaching and practice. The Center is located in 507 Gruening. Call 474-5470 for Speaking Center hours and to schedule an appointment. Please contact me as required should you need to contact other subject matter support services relevant to the development of your leadership or class projects/topics.

Students with Disabilities:

Students with learning or other disabilities who may need special accommodations are encouraged to make an appointment with the Office of Disability Services, http://www.uaf.edu/disability/ (907 474-5655 or TTY at 907 474-1827). Please inform me of any impediments to meeting course objectives which cannot be fully addressed by the Office of Disability Services. I will work with the Office of Disabilities Services (208 Whitaker Bldg) to provide reasonable accommodation to students with disabilities.

	Week	Date	Item	Activity
	Week 1			Class Overview
Historical	Week 2		Assigned	**Term Paper Topic Due Date**
			Topic	History of Cyber Environment
			Reading	
	Week 3		Assessed	**#1 Structured Reflective Journal Comments Due**
			Topic	ARPRANET and Historical Aspects of the Internet
			Reading	
	Week 4		Topic	Cyber as a Doman of Conflict
			Reading	*Flying and Fighting in Cyberspace, The Maxwell Papers* by Convertino, DeMattei, and Knierim
			Reading	*Principles of War for Cyberspace* by Cahanin
Theoretical	Week 5		Assessed	**Term Paper Topic Due**
			Topic	Theoretical Typology of Cyber Domain
			Reading	*Slaying Cyber Dragons: Competing Academic Approaches* by Langø,
	Week 6		Topic	Cybersecurity Strategy
			Reading	*Cyber Strategy of the United States 2015*
			Reading	*@War: The Rise of the Military-Internet Complex* by Harris (chapters 1,2,3,4)
	Week 7		Assessed	**#1 Critical Analysis Due**
			Topic	Cyber Power
			Reading	*The Future of Power* by Nye (chapters 5,6,7)
Application	Week 8		Assessed	**Term Paper Outline Due**
			Topic	Cyber and the Military (attacks and types of denial)
			Reading	*Joint Publication 3012 (R) Cyberspace Operations*
			Reading	*The Future of Power* by Nye (chapter 1,2)
	Week 9		Assessed	**#2 Structured Reflective Journal Comments Due**
			Topic	Economics of Cyber Attacks
			Reading	*Case Study on Target*
	Week 10		Topic	SCADA (Supervisory Control and Data Acquisition) and Cyber Domain
			Reading	*Improving Security for SCADA Control Systems* by Hentea
Application of Knowledge	Week 11		Assessed	**#3 Structured Reflective Journal Comments Due**
			Topic	Laws and Statutes within Cyber Domain
			Reading	*Getting it Right: Protecting American Critical Infrastructure in Cyberspace* by Condron
	Week 12		Assessed	**Term Paper Drafts Due**
			Topic	Cyber Strategic Surprise
			Reading	*@War: The Rise of the Military-Internet Complex* by Harris (chapters 8,9,10,)
			Reading	*Case Study on Russia and Georgia Conflict 2008*
Operational	Week 13		Assessed	**#2 Critical Analysis Due**
			Topic	Cyber Security
			Reading	*@War: The Rise of the Military-Internet Complex* by Harris (chapters 5,6)
Future	Week 14		Assessed	**#4 Structure Reflective Journal Comments Due**
			Topic	Anonymous and their place in the Cyber Domain
			Reading	
	Week 15		Assessed	**Term Papers Due**
			Topic	Future of the Cyber Domain
			Reading	*@War: The Rise of the Military-Internet Complex* by Harris (chapters 13,14)