American Public University System

The Ultimate Advantage is an Educated Mind

School of Security & Global Studies National Security Program NSEC 506 Cyber Policy and Practice in National Security 3 Credit Hours Length: 8 weeks Prerequisite: None

Table of Contents

Instructor Information	Evaluation Procedures
Course Description	Grading Scale
Course Scope	Course Outline
Course Objectives	Policies
Course Delivery Method	Academic Services
Course Resources	Selected Bibliography

Instructor Information

Instructor:	APUS Facilitator
Email:	ctl@apus.edu

Course Description (Catalog)

NSEC 506 Cyber Policy and Practice in National Security (3 credit hours)

This course will provide an overview of current cyber policy and practice for non-practitioners in a national security framework. Students will study the cyber threat environment; laws and policies that govern cyber security; current and historical structure, functions, and capabilities of private and governmental agencies comprising the cyber community; and future trends that affect national security.

Course Scope

Course Scope

- This is a broad-based course that explores the issues and problems relevant to cyberspace facing policymakers. It examines a number of issues such as the nature of cyberspace and its relation to the state, protection of critical infrastructure, deterrence, cybercrime, cyber terrorism and cyber war. We will also take a look at current US policy documents in light of what we have learned about cyber issues. The purpose of this course is to your ability to think critically about cyberspace and its place in the field of national security. The course will begin with a look at the character of cyberspace and end with a comparative look at other state cyber policies.
- The course will assess theories of cyber power within traditional national security theories, strategies and doctrines. It will evaluate cyber as a threat to the state and compare the cyber policies of several great powers. Students will participate in weekly Discussion Forums that correlate to weekly readings. Students will write an analytical research paper, and will write a comprehensive final essay using restricted resources.

Course Objectives

After successfully completing this course, you will be able to

• CO – 1 Assess the importance of cyber to US national security.

- CO 2 Distinguish acts of cyber crime, cyber espionage, cyber terrorism and cyberwar.
- CO 3 Judge the theories of cyber deterrence.
- CO 4 Analyze the cyber policies of other major nation states.
- CO 5 Evaluate US Cyber Policy with respect to national security.

Course Delivery Method

This course delivered via distance learning will enable students to complete academic work in a flexible manner, completely online. Course materials and access to an online learning management system will be made available to each student. Online assignments are due by Sunday evening of the week as noted and include Forum questions (accomplished in groups through a threaded forum), examination, and individual assignments submitted for review by the Faculty Member). Assigned faculty will support the students throughout this eight-week course.

Course Resources

Required Course Textbooks

Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz Eds. *From Cyberspace to Cyberpower: Cyberpower and National Security*, Dulles VA: Potomac Books Inc., 2009.

Required Readings: (Accessible from the weekly reading folders under resources or

http://apus.libguides.com/er.php?course_id=6162)

Brown, Gary and Keira Poellet. "The Customary International Law of Cyberspace," *Strategic Studies Quarterly* 6:3 (2012):126-45. (Access via weekly reading folder under resources)

Denning, D. E. (2015). Rethinking the cyber domain and deterrence. *Joint Forces Quarter*. 2, 8-15. (Access via weekly reading folder under resources)

Department of Defense, *The DOD Cyber Strategy*, (Access via weekly reading folder under resources)

Dunlap Jr., Charles J. Maj Gen (Ret). "Perspectives for Cyber Strategists on Law for Cyber War." *Strategic Studies Quarterly*, (2011): 81-99 (Access via weekly reading folder under resources)

Forsyth, James W. "What Great Powers Make of It: International Order and the Logic of Cooperation in Cyberspace." *Strategic Studies Quarterly* 7:1 (2013) (Access via weekly reading folder under resources)

Hurwitz, Roger. "Depleted Trust in the Cyber Commons." *Strategic Studies Quarterly* 6:3 (2012): 20-45 (Access via weekly reading folder under resources).

Iasiello, E. (2013). Is Cyber deterrence an illusory course of action. *Journal of Strategic Security*, 7(1), 54-67. (Access via weekly reading folder under resources)

Kenney, M. (2015). Cyber-terrorism in a post-stuxnet world. *Orbis*, *59*(1), 111-128. (Access via weekly reading folder under resources)

Libicki, Martin C., *Cyberdeterrence and Cyberwar*, RAND Report, Santa Monica: Rand Corp., 2009, (Access via weekly reading folder under resources)

Libicki, Martin C. "Cyberspace is Not a Warfighting Domain." *I/S A Journal of Law and Policy for the Information Society* 8:2 (2012): 325-40, (Access via weekly reading folder under resources)

Libicki, Martin C. "The Spectre of Non-Obvious Warfare." *Strategic Studies Quarterly* 6:3 (2012): 88 - 101 (Access via weekly reading folder under resources)

Lin, Herbert. "Escalation Dynamics and Conflict Termination in Cyberspace." *Strategic Studies Quarterly* 6:3 (2012): 46 -70 (Access via weekly reading folder under resources)

Mandiant, *APT1: Exposing One of China's Cyber Espionage Units*, (2013) (Access via weekly reading folder under resources)

Schmitt, Michael N. "International Law in Cyberspace: The Koh Speech and the Tallinn Manual Juxtaposed," *Harvard International Law Journal*, 54 (2012) (Access via weekly reading folder under resources)

Whitehouse, *Cybersecurity Strategy and Implementation Plan (CSLIP) for the Federal Civilian Government.* (October, 2015) (Access via weekly reading folder under resources)

Whitehouse, *National Security Strategy*. (2015) (Access via weekly reading folder under resources)

Evaluation Procedures

The course grade is based on the following assessments:

Discussion Forums – 20 percent

Each week, a discussion question is provided and posts should reflect an assimilation of the readings. Students are required to provide a substantive initial post by Thursday at 11:55 pm ET and respond to two or more classmates by Sunday 11:55 pm ET. Forum posts are graded on timeliness, relevance, knowledge of the weekly readings, and the quality of original ideas.

<u>Research Proposal (Research Question, Purpose Statement, and</u> <u>Citation Format Exercise) – 15 percent</u>

The components of this assignment include a research question, a purpose statement, and six sources, at least three of which must be peer-reviewed. The specific research question should relate to a general topic in the course.

<u> Research Paper – 35 percent</u>

Based on the research question assignment in Week Two, the research paper should be no more and no fewer than 10 pages, not including the cover page, the reference list, and any appendices.

Final Assignment – 30 percent

This assignment is a take-home essay assignment to test knowledge and assimilation of the course learning objectives. The exclusive use of required texts and readings is mandatory. No outside sources are allowed. The assignment should be no more eight and no fewer than five pages.

Course Outline

Please see the <u>Student Handbook</u> to reference the University's <u>grading scale</u>.

<u>Week</u>	<u>Topic</u>	Course Objectives	<u>Readings</u>	Assignment
1	Introduction to Cyberspace and National Security Policy	CO – 1 Assess the importance of cyber to US national security.	Readings: Kramer, Franklin D., et.al. (Eds) From Cyberspace to Cyberpower: Cyber Power and National Security, "Introduction" (9 pages); Chapter 1 "Cyberpower and National Security: Policy Recommendations for a Strategic Framework" 3-23 (21 pages); Chapter 2 "Defining the Problem" 24-42 (21	Forum Post #1

			pages): Chapter 3, "Toward a Preliminary Theory of Cyberpower" 43-90 (48 pages).	
1	Understanding the Cyber Domain	CO - 1 Assess the importance of cyber to US national security.	Readings: Kramer, Franklin D. et.al. (Eds) From Cyberspace to Cyberpower: Cyber Power and National Security, Chapter 10 "An Environmental Approach to Understanding Cyberpower" 253-274 (22 pages); Chapter 4 "A Graphical Introduction to the Structural Elements of Cyberspace" 91-112 (22 pages); Chapter 5 "Cyberspace and Infrastructure" 113- 146 (34 pages); Chapter 6 "Evolutionary Trends in Cyberspace" 147-170 (24 pages). Libicki, Martin C. "Cyberspace is Not a Warfighting Domain." I/S A Journal of Law and Policy for the Information Society 8:2 (2012): 325-40, (15 pages) (Accessible via the weekly reading folder within the	Forum Post #2 Assignment #1: Research Proposal - due at the end of week 2

			resources section)	
3	Cyber Crime, Espionage and Terrorism	CO – 2 Distinguish acts of cyber crime, cyber espionage, cyber terrorism and cyberwar.	Readings: Kramer, Franklin D., et.al. (Eds) <i>From Cyberspace to</i> <i>Cyberpower: Cyber</i> <i>Power and National</i> <i>Security</i> , Chapter 18, "Cyber Crime" 415-436 (32 pages); Chapter 19, "Cyber Terrorism: Menace or Myth" 437- 464 (28 pages) Mandiant, <i>APT1:</i> <i>Exposing One of</i> <i>China's Cyber</i> <i>Espionage Units</i> , (2013). Review 1-76. (76 pages) (Accessible via the weekly reading folder within the resources section) Kenney, M. (2015). Cyber-terrorism in a post-stuxnet world. <i>Orbis, 59</i> (1), 111-128. (18 pages) (Accessible via the weekly reading folder within the resources section)	Forum Post #3
4	Cyberwar, Law and Policy	CO – 2 Distinguish acts of cyber crime, cyber espionage,	Readings: Schmitt, Michael N. "International Law in Cyberspace: The Koh Speech and the Tallinn	Forum Post #4

cyber	Manual Juxtaposed,"	
terrorism and cyberwar.	Harvard International Law Journal, 54 (2012). (25 pages) (Accessible via the weekly reading folder within the resources section)	
	Dunlap Jr., Charles J. Maj Gen (Ret). "Perspectives for Cyber Strategists on Law for Cyber War." Strategic Studies Quarterly, (2011): 81-99. (19 pages) (Accessible via the weekly reading folder within the resources section)	
	Kramer, Franklin D., et.al. (Eds) <i>From</i> <i>Cyberspace to</i> <i>Cyberpower: Cyber</i> <i>Power and National</i> <i>Security</i> , Chapter 22 "International Law and Information Operations" 525-542. (18 pages)	
	Brown, Gary and Keira Poellet. "The Customary International Law of Cyberspace," <i>Strategic</i> <i>Studies Quarterly</i> 6:3 (2012):126-45. (20	

			pages) (Accessible via the weekly reading folder within the resources section)	
5	/ber Deterrence	CO - 3 Judge the theories of cyber deterrence.	Readings: Libicki, Martin C., <i>Cyberdeterrence and</i> <i>Cyberwar</i> , RAND Report, Santa Monica: Rand Corp., 2009. 1-73 (Accessible via the weekly reading folder within the resources section) Kramer, Franklin D. et.al. (Eds) <i>From</i> <i>Cyberspace to</i> <i>Cyberpower: Cyber</i> <i>Power and National</i> <i>Security</i> , Chapter 13 "Deterrence of Cyber Attacks" 309-340 (32 pages) Denning, D. E. (2015). Rethinking the cyber domain and deterrence. <i>Joint</i> <i>Forces Quarter</i> . 2, 8- 15. (Accessible via the weekly reading folder within the resources section) Iasiello, E. (2013). Is Cyber deterrence an	Forum Post #5

			illusory course of action. <i>Journal of</i> <i>Strategic Security</i> , 7(1), 54-67. (Accessible via the weekly reading folder within the resources section)	
6	Cyberwar in Practice	CO – 3 Judge the theories of cyber deterrence.	Readings: Libicki, Martin C., <i>Cyberdeterrence and</i> <i>Cyberwar</i> , RAND Report, Santa Monica: Rand Corp., 2009. 117-173 (57 pages) (Accessible via the weekly reading folder within the resources section) Libicki, Martin C. "The Spectre of Non- Obvious Warfare." <i>Strategic Studies</i> <i>Quarterly</i> 6:3 (2012): 88 - 101. (13 pages) (Accessible via the weekly reading folder within the resources section) Lin, Herbert. "Escalation Dynamics and Conflict Termination in Cyberspace." <i>Strategic</i>	Forum Post #6

			Studies Quarterly 6:3 (2012): 46 -70. (25 pages) (Accessible via the weekly reading folder within the resources section)	
7	A Comparative Approach to Cyber Policy and Strategy	CO - 1 Assess the importance of cyber to US national security. CO - 4 Analyze the cyber policies of other major nation states.	Readings: Kramer, Franklin D., et.al. (Eds) From Cyberspace to Cyberpower: Cyber Power and National Security, Chapter 20, "Nation-state Cyber Strategies: Examples from China and Russia" 465-490 (35 pages), Chapter 21, "Internet Governance" 491-524 (34 pages) Forsyth, James W. "What Great Powers Make of It: International Order and the Logic of Cooperation in Cyberspace." Strategic Studies Quarterly 7:1 (2013): 93-113. (21 pages) (Accessible via the weekly reading folder within the resources section) Hurwitz, Roger. "Depleted Trust in the Cyber Commons." Strategic Studies	Forum Post #7 Assignment #2 Research paper due at the end of week 7

			Quarterly 6:3 (2012): 20-45. (16 pages) (Accessible via the weekly reading folder within the resources section)	
8	Evaluating US Cyber Policy	CO - 2 Distinguish acts of cyber crime, cyber espionage, cyber terrorism and cyberwar. CO - 3 Judge the theories of cyber deterrence. CO - 5 Evaluate US Cyber Policy with respect to national security.	Readings: Kramer, Franklin D. et.al. (Eds) From Cyberspace to Cyberpower: Cyber Power and National Security, Chapter 23 "Cyberpower and Critical Infrastructure Protection" 543-556 (13 pages); Chapter 24 "Cyberpower from the Presidential Perspective" 557-562 (6 pages). Department of Defense, The DOD Cyber Strategy, (28pages) (Accessible via the weekly reading folder within the resources section) Whitehouse, Cybersecurity Strategy and Implementation Plan (CSLIP) for the Federal Civilian Government.	Forum Post #8 Assignment due at the end of week 8

	(October, 2015) (21 pages) (Accessible via the weekly reading folder within the resources section) Whitehouse, <i>National Security</i> <i>Strategy</i> . (2015) (Accessible via the weekly reading folder within the resources section)	
--	---	--

Policies

Please see the <u>Student Handbook</u> to reference all University policies. Quick links to frequently asked question about policies are listed below.

Drop/Withdrawal Policy Plagiarism Policy Extension Process and Policy Disability Accommodations

Writing Expectations

Citation and Reference Style

Attention Please: Students will follow the APA 6th Edition as the sole citation and reference style used in written work submitted as part of coursework to the University. Assignments completed in a narrative essay or composition format must follow the citation style cited in the *Publication manual of the American Psychological Association* (2009). (6th ed.).

All written submissions should be submitted in Times New Roman 12 pt font with 1" margins, typewritten in double-spaced format. Graduate-level work is expected to be free of grammar, usage, and style errors.

It is very important that students are aware of and comply with the APUS policy on plagiarism in the Student Handbook. To find the plagiarism policy, go to the vertical toolbar in the classroom and click "Policy."

Citation and Reference Style

Attention Please: Students will follow the APA Format as the sole citation and reference style used in written work submitted as part of coursework to the University. Assignments completed in a narrative essay or composition format must follow the citation style cited in the APA Format.

Late Assignments

Students are expected to submit classroom assignments by the posted due date and to complete the course according to the published class schedule. As adults, students, and working professionals, I understand you must manage competing demands on your time. Should you need additional time to complete an assignment, please contact me before the due date so we can discuss the situation and determine an acceptable resolution. Routine submission of late assignments is unacceptable and may result in points deducted from your final course grade.

<u>Netiquette</u>

Online universities promote the advancement of knowledge through positive and constructive debate – both inside and outside the classroom. Forums on the Internet, however, can occasionally degenerate into needless insults and "flaming." Such activity and the loss of good manners are not acceptable in a university setting – basic academic rules of good behavior and proper "Netiquette" must persist. Remember that you are in a place for the rewards and excitement of learning which does not include descent to personal attacks or student attempts to stifle the Forum of others.

• **Technology Limitations:** While you should feel free to explore the full-range of creative composition in your formal papers, keep e-mail layouts simple. The Sakai classroom may not fully support MIME or HTML encoded messages, which means that bold face, italics, underlining, and a variety of color-coding or other visual effects will not translate in your e-mail messages.

Humor Note: Despite the best of intentions, jokes and <u>especially</u> satire can easily get lost or taken seriously. If you feel the need for humor, you may wish to add "emoticons" to help alert your readers: ;-), :),

Disclaimer Statement

Course content may vary from the outline to meet the needs of this particular group.

Table of Contents

Online Library

The Online Library is available to enrolled students and faculty from inside the electronic campus. This is your starting point for access to online books, subscription periodicals, and Web resources that are designed to support your classes and generally not available through search engines on the open Web. In addition, the Online Library provides access to special learning resources, which the University has contracted to assist with your studies. Questions can be directed to <u>librarian@apus.edu</u>.

- **Charles Town Library and Inter Library Loan:** The University maintains a special library with a limited number of supporting volumes, collection of our professors' publication, and services to search and borrow research books and articles from other libraries.
- **Electronic Books:** You can use the online library to uncover and download over 50,000 titles, which have been scanned and made available in electronic format.
- **Electronic Journals:** The University provides access to over 12,000 journals, which are available in electronic form and only through limited subscription services.
- **Tutor.com**: AMU and APU Civilian & Coast Guard students are eligible for 10 free hours of tutoring provided by APUS. <u>Tutor.com</u> connects you with a professional tutor online 24/7 to provide help with assignments, studying, test prep, resume writing, and more. Tutor.com is tutoring the way it was meant to be. You get expert tutoring whenever you need help, and you work one-to-one with your tutor in your online classroom on your specific problem until it is done.

Request a Library Guide for your course (<u>http://apus.libguides.com/index.php</u>)

The AMU/APU Library Guides provide access to collections of trusted sites on the Open Web and licensed resources on the Deep Web. The following are specially tailored for academic research at APUS:

- Program Portals contain topical and methodological resources to help launch general research in the degree program. To locate, search by department name, or navigate by school.
- Course Lib-Guides narrow the focus to relevant resources for the corresponding course. To locate, search by class code (e.g., SOCI111), or class name.

If a guide you need is not available yet, please email the APUS Library: <u>librarian@apus.edu</u>.

Table of Contents

Turnitin.com

Faculty may require assignments be submitted to Turnitin.com. Turnitin.com will analyze a paper and report instances of potential plagiarism for the student to edit before submitting it for a grade. In some cases professors may require students to use Turnitin.com. Typically the course professor will establish a Turnitin.com access code for his/her classes. If the code has not been established, those who wish to use Turnitin.com may ask their professor to establish the code.

Selected Bibliography

Table of Contents