American Public University System

The Ultimate Advantage is an Educated Mind

School of Security and Global Studies
INTL440 Cyber Warfare
Credit Hours: 3
Length of Course: 8 Weeks
Prerequisite: NONE

Table of Contents

Course Description (Catalog)

This course provides an overview of cyber warfare and the potential impact of its use by military, terrorist, and criminal organizations. By studying the operation of computer networks, the student will gain an appreciation of how they have both benefited society and made portions of its infrastructure more vulnerable. An overview of cyber weaponry will be presented, and various offensive and defensive strategies will be examined via case studies.

Table of Contents

Course Scope

As a 400-level course, this course provides a higher level of knowledge building on the material taught at the 300 level. The purpose and scope of

this course is to enable the student to build a deeper understanding of the discipline.

Table of Contents

Course Objectives

After successfully completing this course, you will be able to:

CO-1: Analyze cyberspace and cyber warfare.
CO-2: Diagram basic computer network operations.
CO-3: Compare selected cyber weapons and their associated attack strategies.
CO-4: Examine defensive strategies for securing networks.
CO-5: Evaluate cyber war capabilities of selected nations.

Table of Contents

Course Delivery Method

This course, delivered via distance learning, will enable students to complete academic work in a flexible manner, completely online. Course resources and access to an online learning management system will be available to each student. Online assignments are due by Sunday at 11:55 pm ET and include all written assignments, examinations, and research papers submitted for grading. Weekly Forum questions (accomplished in groups in a Forum) require an initial response by Thursday at 11:55 pm ET, with all other required responses due by Sunday at 11:55 pm ET. The assigned faculty will support the students throughout this eight-week course.

Table of Contents

Course Resources

Required Course Textbook:

- Chapple, Mike, and David Seidl. *Cyberwarfare: Information Operations in a Connected World*. Burlington, MA: Jones & Bartlett Learning, 2015.

- External websites and other assigned reading found in the Lessons area of the classroom.

- Weekly Lesson Notes and videos or audio files are found in the Lessons area of the classroom.

Table of Contents

Evaluation Procedures

Forum discussions – 25 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 2 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.

Midterm assignment - 25 percent

This assignment is a take-home essay assignment of 2 questions, 3 pages each, to test knowledge and assimilation of the course objectives. The exclusive use of required texts and readings from this course is mandatory.

Progress assignment - 25 percent

Specialized Exercise. 8-10 pages including research and analysis.

Final assignment – 25 percent

This assignment is a take-home essay assignment of 2 questions, 3 pages each, to test knowledge and assimilation of the course objectives. The exclusive use of required texts and readings from this course is mandatory.

Grade Instruments	Percentage
Forum Discussions (8)	**25**
Progress Assessment	**25**
Midterm Assessment	**25**
Final Assessment	**25**
Total	**100**

Table of Contents

8 – Week Course Outline

Week 1: What is Cyber Warfare

Learning Outcomes:
CO-1: Analyze cyberspace and cyber warfare

Assignments: Complete all required forums.

Required Readings:

Chapple, Mike, and David Seidl. 2015. *Cyberwarfare: Information Operations in a Connected World*. Burlington, MA: Jones & Bartlett Learning. Chapters 1 and 8.

Clapper, James R. 2015. *Worldwide Cyber Threats*. House Permanent Select Committee on Intelligence.

Hildick-Smith, Andrew. 2005. "Security for Critical Infrastructure SCADA Systems." Sans Institute.

Libicki, Martin C. 2009. "Cyberdeterrance and Cyberwar." *RAND Project Air Force*. Pages 1-114.

The White House. 2010. "The Comprehensive National Cybersecurity Initiative." https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative.

Recommended Optional Readings:

U.S. Strategic Command. "U.S. Cyber Command Factsheet." https://www.stratcom.mil/factsheets/2/Cyber_Command/

FBI. "National Cyber Investigative Joint Task Force." http://www.fbi.gov/about-us/investigate/cyber/ncijtf

Symantec http://www.symantec.com/

McAfee http://www.mcafee.com/us/mcafee-labs.aspx

Schneier on Security. *Crypto-Gram Newsletter.* https://www.schneier.com/crypto-gram/

The Shadowserver Foundation. http://www.shadowserver.org/wiki/pmwiki.php/Shadowserver/Mission

Week 2: Potential Targets

Learning Outcomes:
CO-1: Analyze cyberspace and cyber warfare

Assignments: Complete all required forums.

Required Readings:

"Can Hackers Turn Your Lights Off? The Vulnerability of the US Power Grid to Electronic Attack." 2001. SANS Institute.

Chapple, Mike, and David Seidl. 2015. *Cyberwarfare: Information Operations in a Connected World*. Burlington, MA: Jones & Bartlett Learning. Chapter 2.

Gardels, Nathan. 2011 "Mike McConnell: An American Spymaster on Cyberwar." *The Huffington Post*.

Gasper, Peter D. 2008. "Cyber Threat to Critical Infrastructure 2010-2015: Increased Control System Exposure." Idaho National Laboratory.

Lawson, Shannon M. 2002. "Information Warfare: An Analysis of the Threat of Cyberterrorism Towards the US Critical Infrastructure." SANS Institute.

Office of the National Counterintelligence Executive. 2011. "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on *Foreign Economic Collection and Industrial Espionage, 2009-2011*."

Week 3: Cyber Weapons

Learning Outcomes:
CO-2: Diagram basic computer network operations.
CO-3: Compare selected cyber weapons and their associated attack strategies.

Assignments: Complete all required forums and progress assessment.

Required Readings:

Chapple, Mike, and David Seidl. 2015. *Cyberwarfare: Information Operations in a Connected World*. Burlington, MA: Jones & Bartlett Learning. Chapter 7.

Poulin, Martin. 2006. "Hacking: The Basics." SANS Institute.

Skoudis, Ed. "Top 15 Malicious Spyware Actions." SANS Institute.

Robb, John. 2007. "When Bots Attack." *Wired Magazine,* Issue 15-09 (Aug 23).

Recommended Optional Readings:

Security Week. http://www.securityweek.com

Symantec. http://www.symantec.com

Week 4: Cyber Tactics

Learning Outcomes:
CO3**:** Compare selected cyber weapons and their associated attack strategies.

Assignments: Complete all required forums.

Required Readings:

Allen, Malcolm. 2006. "Social Engineering: A Means to Violate a Computer System." SANS Institute.

Chapple, Mike, and David Seidl. 2015. *Cyberwarfare: Information Operations in a Connected World*. Burlington, MA: Jones & Bartlett Learning. Chapters 5 and 6.

Robinson, Shane W. 2007. "Corporate Espionage 201." SANS Institute.

Thomas, Timothy L. 2008. "Cyberskepticism: The Mind's Firewall." U.S. Army Foreign Military Studies Office. (Spring).

Week 5: Cyber Defense

Learning Outcomes:
CO4**:** Examine defensive strategies for securing networks.

Assignments: Complete all required forums and the midterm assessment.

Required Readings:

Chapple, Mike, and David Seidl. 2015. *Cyberwarfare: Information Operations in a Connected World*. Burlington, MA: Jones & Bartlett Learning. Chapters 11, 12, and 13.

Hildick-Smith, Andrew. 2005. "Security for Critical Infrastructure SCADA Systems." Sans Institute.

Libicki, Martin C. 2009. "Cyberdeterrance and Cyberwar." RAND Project Air Force. Pages 1-114.

The White House. 2010. "The Comprehensive National Cybersecurity Initiative." https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative.

Recommended Optional Readings:

U.S. Strategic Command. "U.S. Cyber Command Factsheet." https://www.stratcom.mil/factsheets/2/Cyber_Command/

Week 6: Case Studies I

Learning Outcomes:
CO5**:** Evaluate cyber war capabilities of selected nations.

Assignments: Complete all required forums.

Required Readings:

Chapple, Mike, and David Seidl. 2015. *Cyberwarfare: Information Operations in a Connected World*. Burlington, MA: Jones & Bartlett Learning. Chapter 4.

Krekel, Bryan. 2009. "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," prepared by Northrop Grumman for *The US-China Economic and Security Review Commission.*

Thomas, Timothy L. 2010. "Google Confronts China's 'Three Warfares.'" *Parameters*. (Summer).

Thornbaugh, Nathan. 2005. "The Invasion of the Chinese Cyberspies: An Exclusive Look at How the Hackers called TITAN RAIN are stealing U.S. Secrets." *Time* (29 Aug).

Wortzel, Larry M. 2010. "China's Approach to Cyber Operations: Implications for the United States." Testimony before the Committee on Foreign Affairs, House of Representatives.

Recommended Optional Readings:

"The Dark Visitor - Inside the World of Chinese Hackers." www.thedarkvisitor.com.

Center for Strategic and International Studies Selected Bibliography for Cybersecurity. 2011. https://www.csis.org/analysis/selected-bibliography-cyber-security.

Week 7: Case Studies II

Learning Outcomes:

CO5**:** Evaluate cyber war capabilities of selected nations.

Assignments: Complete all required forums.

Required Readings:

Chapple, Mike, and David Seidl. 2015. *Cyberwarfare: Information Operations in a Connected World*. Burlington, MA: Jones & Bartlett Learning. Chapters 9 and 10.

Davis, Joshua. 2007. "Hackers Take Down the Most Wired Country in Europe." *Wired*, (21 August).

Gates, Guilbert. 2012 "How a Secret Cyberwar Program Worked." *The New York Times* (1 June).

Harlan, Chico and Ellen Nakashima. 2011. "Suspected North Korean Cyberattack on a Bank Raises Fears for South Korea, Allies." *The Washington Post* (29 August).

Lewis, James A. 2009. "The "Korean" Cyber Attacks and Their Implications for Cyber Conflict." *Center for Strategic and International Studies* (October).

Prevelakis, Vassilis and Diomidis Spinellis. 2007. "The Athens Affair." *IEEE Spectrum* (July).

Sanger, David E. 2012. "Obama Order Sped Up Wave of Cyberattacks Against Iran." *The New York Times* (1 June).

Sverdlove, Henry. 2010. "Stuxnet Worm Shows Critical Infrastructure Attacks No Longer Just Hollywood Hype." *SC Magazine* (18 October).

Recommended Optional Readings:

Langner Communications. http://www.langner.com/english.

Sin, Steve. 2009. "Cyber Threat posed by North Korea and China to South Korea and US Forces." *Start* 364: 28-33.

Week 8: Future of Cyber Warfare, Course Reflection and Review

Learning Outcomes:
CO-1: Analyze cyberspace and cyber warfare.
CO-2: Diagram basic computer network operations.
CO-3: Compare selected cyber weapons and their associated attack strategies.
CO-4: Examine defensive strategies for securing networks.
CO-5: Evaluate cyber war capabilities of selected nations.

Assignments: Complete all required forums and the final assessment.

Required Readings:

Chapple, Mike, and David Seidl. 2015. *Cyberwarfare: Information Operations in a Connected World*. Burlington, MA: Jones & Bartlett Learning. Chapters 3, 14 and 15.

Table of Contents

Policies

Please see the Student Handbook 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

Citation and Reference Style

Attention Please: Students will follow the Turabian/Chicago Style as the sole citation and reference style used in written work submitted as part of coursework to the University.
See http://www.apus.edu/Online-Library/tutorials/chicago.htm.

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.

Deductions:
Late forum posts can be penalized up to 5 points per day
Late assignments can be penalized up to 5 points per day

Netiquette

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 especially 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: ;-), :), ☺

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 **librarian@apus.edu**.

- ***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. Tutor.com 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 (http://apus.libguides.com/index.php)

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: librarian@apus.edu.

Table of Contents