ED 504
Understanding Adversaries and Threats to the United States and to the Department of Defense

SAMPLE COURSE SYLLABUS*

1. Introduction

Understanding Adversaries and Threats to the United States and to the Department of Defense (ED 504) is an advanced, semester-long course that will facilitate a deeper understanding and appreciation of the major threats to the United States and to the DoD and to explore strategies for identifying and evaluating those threats. An integral part of a coordinated program of graduate-level professional education for security professionals, ED 504 will challenge students to think more systematically about the impact of enduring and emerging adversaries and threats, an essential skill for progressive development as future leaders of the Department of Defense (DOD) security enterprise.

The 16-week course, which equates to three credit hours, contains material up to the SECRET classification level and will be conducted via the Sakai Collaborative Learning Environment (CLE). Instructional methods and will consist of readings, prerecorded lectures and presentations, online primarily asynchronous sessions and collaboration through a discussion forum, student collaboration and student written assignments. Specific prerequisites for this course are:

- Online course Establishing an Insider Threat Program for Your Organization CI122.06
- Online course Insider Threat Awareness Course CI121.06
- Online course “Derivative Classification” (IF103.16)
- Online course “Marking Classified Information (IF105.16)

2. Course Description/Overview

The challenges facing security professionals grow more complex daily: the threat of terrorists against the homeland and U.S. interests abroad, the proliferation of dangerous advanced technologies, and the impact of increasing globalization in all its forms. The focus of ED504 is on those threats, both foreign and domestic, from a strategic perspective: foreign intelligence services, non-governmental entities such as international crime and global terrorist networks; and other adversaries and threats from a strategic. The course objectives center on understanding the complexities of those challenges as well as allocating resources most prudently in an uncertain world. Using its “macro-look” at the spectrum of enduring and emerging threats as appoint of departure, students will analyze, synthesize and evaluate the lessons from to be learned from history to address such questions as: “Who are our adversaries?” “What are their intentions, capabilities, methods and modes of operation?” and “What are the vulnerabilities that may provide opportunities for counter-action?”

*Sample syllabus is subject to change each semester.

3. Student Outcomes/Objectives

At the end of the course, students should be able to:

1. Summarize, compare and contrast the enduring and emerging threats to the United States and the implications for the DOD security mission.
2. Analyze the threats to national security posed from external actors; the foreign governments both friendly and adversarial that collect against the United States and the methods of operation of their intelligence services
3. Analyze the threats to national security posed from external non-state, foreign actors, including terrorist groups, and their methods of operation
4. Analyze the threats to national security posed from domestic actors
5. Analyze the challenges to security professionals from the proliferation of nuclear, chemical and biological weapons of mass destruction
6. Analyze the challenges to security professionals from the proliferation of modern conventional weaponry, and advanced technologies
7. Analyze the threats to national security posed from the hostile use of information technologies; cyber attack and cyber espionage
8. Analyze the challenges to security professionals from both government and industrial espionage with reference to specific cases
9. Evaluate the impact of potential threats on vulnerable components of the national infrastructure, such as water, transport, energy, food, finance, and industry
10. Analyze the differences and similarities of deliberate, hostile threats from those from natural causes
11. Recognize the roles, responsibilities, capabilities/statutory authorities and limitations of the agencies comprising the Intelligence Community
12. Apply the principles and process of the intelligence cycle to request threat assessments from the appropriate intelligence, counterintelligence, and law enforcement activities
13. Evaluate the benefits, costs and risks associated with counter-intelligence and covert action as means of national security
14. Analyze the significant threats to a specific program, operation, installation or organization, and the alternatives to identify and mitigate those threats
15. Evaluate possible security measures to reduce risks associated with specific threats, including the proactive (i.e., preventive) best practices to mitigate a specific type of threat in a real or hypothetical organization

4. Course Materials

The following texts will be used in whole or in part during the course:

University of Chicago (2010). *The Chicago Manual of Style* (16th Ed.). Chicago: Univ. of Chicago Press. ISBN 9780226104201.

Homeland Security and Terrorism, Readings and Interpretations, Russell Howard, James Forest, Joanne Moore, ***1st edition***, 2006.

Intelligence: From Secrets to Policy, 5th Edition, Mark M. Lowenthal, 2012.

Capturing Jonathan Pollard, Ronald J. Olive, 2006.

Grave New World: Security Challenges in the 21st Century, edited by Michael E. Brown, Georgetown University Press, 2003.

Seeking Security in an Insecure World, Dan Caldwell, Robert E. Williams, Jr Rowman & Littlefield, (second edition, 2012).

Other unclassified and classified readings and references will be provided electronically (text or URL) and will include:

The Farewell Dossier: Duping the Soviets Gus Weiss (Studies in Intelligence).

US National Intelligence: An Overview (213)
http://www.odni.gov/files/documents/USNI%202013%20Overview_web.pdf

Worldwide Threat Assessment of the U.S. Intelligence Community for the Senate Armed Services Committee DNI April 18, 2013.
http://www.odni.gov/files/documents/Intelligence%20Reports/SASC%20WWTA%20Remarks%20as%20delivered%2018%20April%202013.pdf

CI Targeting U.S. Technologies: A Trend Analysis of Reporting from Defense Industry (2013 Unclassified and SECRET editions).
http://www.dss.mil/documents/ci/2013%20Unclass%20Targeting%20US%20Technologies_FINAL.pdf

Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage

The Crimson Shield (a new monthly classified report released by DSS CI documenting significant counterintelligence, intelligence, and security-related issues relevant to the cleared contractor community –available on the DSS SIPRNET web site https://www.dss.smil.mil).

Can't We All Just Get Along? Improving the Law Enforcement-Intelligence Community Relationship National Defense Intelligence College June 2007.

The Department of Homeland Security Intelligence Enterprise: Operational Overview & Oversight Challenges for Congress Mark Randol CRS R 40602 2010.

*Report to the Congress on Foreign Economic and Industrial Espionage 2009-2011.*NCIX 2011.

The Movie Breach: A Personal Perspective, Studies in Intelligence Vol 52, No 1, 2008 Brian Kelley.

Silber and Bhatt *Radicalization in the West: the Homegrown Threat* NYPD

5. Student Requirements

The course will consist of readings, class participation, research papers, and student presentations, and evaluations. Written assignments will be submitted **(unless otherwise noted) by midnight Eastern Time, Sunday of the week that they are assigned**. (Note: the final paper is due midnight Wednesday of Week 16).In the event of a serious problem, students should contact the instructor in a timely fashion, before the due date. Unexcused late submissions will be penalized 10% of the possible points for that activity for each week late. Assigned readings are from both non-governmental sources, e.g. academic/research products, industry and journalism; and government publications such as legislation, executive orders, policies, plans, and strategies and derivative implementation guidance, and reviews from the Government Accountability Office, Congressional Research Service, and the executive branch. Students are expected to familiarize themselves with the assigned topic and readings each week and should be prepared to discuss and debate them critically, as well as analyze them for biases and multiple perspectives. Assignments, quizzes and collaborative small-group activities are based on the assumption of completion of all readings assigned for the course.

Two Short Papers (20%)

The first paper, worth 13% of the final grade and due midnight, Sunday Week / Lesson 7, will be a critical book review of Olive's *Capturing Jonathan Pollard.* The format should be: length of 4-5 pages, double-space, 'Times New Roman' 12 point font. Title page, references and bibliography will not be included as part of the page count. "*Critical*" thinking means making some analytical judgment as to the validity or merit of his conclusions, but not necessarily one that is harsh or unfavorable. Students will be directed to reflect carefully on the material with reference to their selected organizational theme, summarize clearly and concisely Olive's message, and then evaluate how well he makes his case, the strength of his evidence and analysis, and the validity of his assumptions. They will be expected to ground their analysis securely with specific citations from the text, supported by reference to at least three other course references. Their analysis will focus on what Olive suggests are the human and systemic errors that enabled Pollard's actions, and then conclude with their own judgment on what single factor is most relevant to prevent a similar breakdown of security in their own organization.

The second paper, worth 7% of the final grade and due by midnight Sunday of the week/ lesson 11, is a background paper of 2-3 pages on the most important lessons to be learned from the "Farewell" counterintelligence case. (Note: A background paper is most commonly used on a staff to summarize the information underlying an issue or subject.)
A short introduction will present the purpose and basic "road map" for the paper, followed by cohesive, single-idea content paragraphs to lead the reader logically to the conclusion. Start with the header "BACKGROUND PAPER" 1 inch from the top of the first page and three lines above text and use a 1-inch margin all around, double space.
Include your name, organization, office symbol, and phone number on the first page 1 inch from the bottom of the page.). The key to an effective background paper, like any well-written

document, is to get to the point quickly, cover all aspects of the issue in sufficient detail to meet your objective, and close the paper with a sense of finality.

Long Research Paper (40%)

The long research paper will be an individual analysis of all the significant threats to a specific real-world program, operation, installation or organization (of the students' choosing), and of the alternatives to identify and mitigate those threats. Students should mine available information sources to determine the key adversary, its capabilities, intentions, organization, mode of action, partners (if any) and long range prospects. Then students will be expected to apply the principles and process of the intelligence cycle to suggest what the threat assessments should be requested from the appropriate intelligence, counterintelligence, and law enforcement activities, and to determine the gaps in essential information to be used to generate new requirements for collection and analysis. They will evaluate the alternative possible security measures to reduce risks associated with those specific threats, including the proactive (i.e., preventive) best practices to mitigate a specific type of threat in a real or hypothetical organization. Their calculus should encompass an evaluation of the benefits, costs and risks associated with counter-intelligence activities and covert action that might be considered as part of the recommended course of action. A graded (10% of the paper's grade) initial annotated bibliography of at least twelve sources is due on week 5. The papers may be classified up to SECRET.

The paper shall be **12-15** pages, double space, 'Times New Roman' 12 point font. Title page, references and bibliography are not included in the page count. Use the Chicago Manual of Style citation style, using endnotes with proper citation, minimizing discursive text within the notes, and a separate bibliography. The proposed subject (program, operation, installation or organization) will be submitted for approval at the start of Week 2, an annotated bibliography by Week 5 and final draft is due by midnight **Wednesday** of Week 16.

Quizzes (16%)

There will be two Sakai administered short answer open book quizzes during the course. Each will be worth 8 percent of overall grade. Quizzes will be assigned at lessons 3 and 12 to be completed and submitted by the end of lessons 8 and 15 respectively; each to be graded/reviewed to ensure student understanding of problem areas or need for further work. One question on each quiz (eachworth 3% of the final grade) will require classified research and a separate response using SIPRnet.

Class Participation (24%)

Participation, which is important and required, includes making inputs to the class discussion forum, participating in small-group exercises, and reflecting on the class experience by recording their thoughts weekly with the professor and their fellow students via email or chat room. For full credit, student comments to all weekly discussion prompts and responses to at least one other student's discussion posts each week, should be thoughtful, relevant (to the lesson), substantive, clear, concise (3 to 5 lines would generally be adequate) and grammatically correct. Responses to all of the lesson discussion questions, and initial comments on the readings, should be posted not later than midnight (Eastern Time) Friday of the lesson week. Comments on at least one other student's response to each question are due not later than midnight (Eastern Time) of that Sunday. If, due to an emergency, students are not able to respond to a discussion prompt in the week it is assigned, they must contact the instructor by e-mail and will be expected to post their response in the following week.

6. Grading

The course's graded activities are weighted as follows:

Assignments	Course Percentage	Points
Discussion Forum Participation*	24%	120
Short Papers (2 at 13 and 7%)	20%	100 (65 and 35)
Quizzes (2 at 8% each)	16%	80
Long research paper	40%	200
Total points	100%	500

Written assignments will be graded following the rubric and the criteria below:

Element Evaluated	Evaluation Criteria			
	A-Excellent 90-100%	B-Good 80-89%	C-Below Standards 70-79%	D/F Failure 69 or below%
Content of paper, analysis, (50% of paper's grade of which 10% is for Annotated bibliography)	Critical thinking related to the issues, substance, points raised and arguments presented is very evident	Critical thinking is well demonstrated	Some critical thinking is shown but could improve	Critical thinking is not well demonstrated or not evident
Application of theory and knowledge to given facts (20%)	Application of theory and knowledge is very evident	A good understanding of theory and knowledge is shown	Some understanding of theory and knowledge is shown	Understanding of theory and knowledge is lacking in significant respects or absent

Element Evaluated	Evaluation Criteria			
Completeness (15%)	Assignment is complete in every aspect and exceeds requirements	Assignment is complete	Assignment is mostly complete but missing some required elements	Assignment is missing major elements
Terminology (5%)	Use of terminology is correct in all instances	Terminology is mostly correct	Multiple mistakes in terminology	Correct terminology not used
Organization / Style (10%) Form (grammar, format, punctuation, spelling, logic) citation)	Organization is relevant to topic, clear and understandable with logical flow Virtually error free.	Mostly relevant, clear, and logical Few errors (one per page or less)	Unclear, Lacks relevance, is difficult to understand, or logic is missing. Frequent Errors (over one per page)	Disorganized, improper style. Form errors endemic throughout.

***Class Participation**: Students' online participation will be evaluated based on the following criteria:

Content – Evidence of critical thinking relative to the issues, substance, points raised, and arguments presented.
Terminology – Proper use of technical concepts introduced in the course readings and discussions and appropriate to this area of study.
Application – How the student applies theories and knowledge to given facts.
Complete Response – Answering all questions asked and sub-questions inferred.
Organization/Style – Relevance to topic, clarity, understandable, logical flow.
Grammar/Mechanics – Citations, punctuation, spelling, proper word usage.

Class participation will be graded in the following manner:

Percentage	Grading Rubric
A Excellent = 90-100% (108-120 pts)	Participates in 90% or more of Discussions and all Assignments. Contributes concisely, thoughtfully and substantively to each topic.
B Good = 80-89% (96-107 pts)	Participates in all least 75% of Discussions and all Assignments. Contributes substantively to most topics.
C Below Standards = 70-79% (84-95 pts)	Participates in less than 75% of Discussions and all Assignments. Contributes substantively to the

	topics
D/F Failure = 69 or below (0--83 Pts)	Participates in less than 65% of Discussions and Assignments. Contributes little or not at all to the topics. . (Note also that even if late, substantive and concise comments can recapture the majority of the participation points).

Notwithstanding the incremental grades achieved in various graded elements of the course (i.e. papers, quizzes, and participation), the standard of success at the graduate level is predicated on a cumulative score of 80% or higher. Individual graded assignments with a score lower than 80% are acceptable; however, a student's final grade at the end of the semester must be 80% or higher to pass the course. The final course grade will be based on the following cumulative points earned:

Letter Grade	**Point Range**
A = 90% - 100%	450 points or higher
B = 80% - 89%	400-449 points
C = 70% - 79%	350-399 points
F = 69% and below	349 and below

A final numeric (percentage) score for each student who completes the class and the dates of attendance will be recorded in the student's training record in CDSE's "STEPP" learning management system. The record in STEPP will also indicate that students who achieve a final score of 80% or higher passed the course.

7. Academic Integrity and CDSE Plagiarism Policy

The Center for Development of Security Excellence holds its students, faculty and staff to the highest standards of integrity and security. The Center does not tolerate the misleading use of any information and data bearing in mind that the CDSE is an institution that allows and encourages its students to conduct classified research. All alleged violations of academic integrity will be investigated and resolved. The CDSE specifically prohibits plagiarism, defined as the act of taking ideas, writings, or the like from another and passing them off as one's own by not providing the proper credit to the original author. Specifically, it is the intentional, knowing, or reckless failure to document or correctly attribute another's ideas. Plagiarism includes, but is not limited to the duplication of an author's words without both quotation marks and accurate references or footnotes and/or use of an author's ideas in paraphrase without accurate reference or footnotes. Students are expected to credit properly and accurately the source of materials directly cited or indirectly used (i.e., paraphrased) in any oral or written work. All student work shall be their own, unless otherwise properly noted. Students may not use entire papers, or substantive selections of a paper for one course, to complete work for another course or courses, although students may, with an instructor's prior permission, use up to a maximum of 25% of a paper for another course's paper requirement, and it must be clearly footnoted as such. However, students may use sections, or entire parts, of course papers in their thesis without annotation or footnoting.

See the Weekly Agenda for Detailed Lessons