Course Overview

Intensive study in specific areas of homeland security and cybersecurity with regards to nation-state cyberwarfare and terrorism. This course addresses the challenges involved in information warfare and information security as it pertains to domestic and international security challenges. This semester's course will focus on state-sponsored as well as transnational cyber-warfare and touch briefly on industrial espionage.

Homeland Security encompasses a grouping of diverse missions and functions that are performed by a wide variety of organizations on the local, state, federal and international levels. Cyber Security is a very young and poorly understood realm within Homeland Security, and there are many definitions for what is and what is not cyber security. This niche is very rapidly evolving and it is likely that material presented in this semester will no longer be interesting in future semesters. Given our time allowance within fifteen weeks, what we will cover in this course are few key examples that best exemplifies the study of cyber security.

The purpose of this class is NOT to train the student in "how to hack computers." True cyber security information warriors hone their craft over decades in traditional education, chat rooms, conferences, and hacking competitions. You will not leave this course a better computer hacker than when you started. You will, however, be a more informed participant of the Internet and can use this new depth of knowledge to pursue opportunities in CNA/CND or IA (computer network attack, computer network defense, information assurance). You will learn how to discern plausible cyber security threats from the improbable. And you will learn the current state of what is possible with cyber attack, attribution, defense, and policy.

By the end of the course you are expected to demonstrate six cognitive learning skills:

- **Knowledge**: Recall data or information.
- **Comprehension**: Understand the meaning, translation, interpolation, and interpretation of instructions and problems. State a problem in one's own words.
- **Application**: Use a concept in a new situation or unprompted use of an abstraction. Applies what was learned in the classroom into novel situations in the work place.
- **Analysis**: Separates material or concepts into component parts so that its organizational structure may be understood. Distinguishes between facts and inferences.
- **Synthesis**: Builds a structure or pattern from diverse elements. Put parts together to form a whole, with emphasis on creating a new meaning or structure.
- **Evaluation**: Make judgments about the value of ideas or materials.

The assignments for this course are designed to assess the ability of the student to demonstrate these cognitive learning skills.

Course Structure and Conduct

- In-class lecture and discussion about the readings
- Individual weekly written responses to the readings
- Online commenting on contemporary news and blog postings
- Final exam consisting of a cybersecurity policy paper
Enrollment Information

- Homeland Security graduate student
- Or Open University student, per Instructor's approval

Course Materials

- Personal computer with high-speed Internet access at home
- Clifford Stoll, The Cuckoo's Egg
- Mark Bowden, Worm
- Kevin Poulsen, Kingpin
- Joel Brenner, Glass Houses
- Richard Clarke, Cyber War
- Thomas Rid, Cyber War Will Not Take Place

Course Assessment and Grading

- 30% In-Class Participation
- 20% Online Participation
- 15% Final Exam (Cybersecurity Policy Paper)
- 35% Weekly written responses to readings

Other Course Policies

All students enrolled in this course must understand the following requirements and responsibilities and adhere to the course policies. These policies and requirements are intended to ensure an informative and enjoyable experience for students and the instructor. Read the following carefully, ask clarifying questions, and consider your enrollment in this course thoughtfully.

If a student does not agree with the policies, responsibilities, and requirements of this course, the student must drop the course immediately and stop attending class discussions. Continued enrollment, attendance, and participation in the course implicitly indicates a student's agreement with the following policies, responsibilities, and requirements.

Technical Requirements

Students must have reliable, regular, and affordable access to a high-speed Internet connection and a personal computer. It is best if both these items are accessible at home, but SDSU students are fortunate enough to have access to the Student Computing Center (300 PCs and 36 Mac). Laptop computers or tablets are completely optional but are strongly encouraged. If you are fortunate enough to have a tablet or laptop, consider bringing it to class.

Technical Proficiency

Students must obtain or maintain technical proficiency with the following technologies. In the event that the student is unfamiliar or uncomfortable with technologies, the student is responsible to seek training from the appropriate campus resources, the instructor, or elsewhere. This proficiency should be achieved within the first week of class. Continued participation in this course will assume your proficiency with the following:

- Personal Computers: Mac or PC
- Web Browser: Chrome, Firefox, Safari, Internet Explorer, etc.
- Email: Gmail, Yahoo Mail, Hotmail, Outlook, OS X Mail, Rohan, etc.
- Email Filters: the ability to direct certain messages to folders for later review
- Word Processor: Microsoft Word, Apple Pages, Google Docs, OpenOffice, etc.
- PDF Viewer: OS X Preview, Acrobat Reader (version X or above), Foxit Reader, Nitro Reader
- Interactive Websites: also known as "Web2.0", online banking, Facebook, webmail, etc.
- Blogs: viewing, commenting, and navigating online information "web logs"

Students should regularly access and interact with the course collaboration portal which provides online discussion, collaboration, and assignment submission capabilities. While there is no minimum number of logins required, successful students would average 3-4 logins per week. Students are required to review any content
posted online, as it becomes an integral part of our community discussion and serves to inform the student about contemporary topics.

Email Notifications
To remove the burden of checking the portal repeatedly, email notifications will be sent out for every new discussion, comment, file, task, or assignment posted to the website. It is very important that students maintain accurate contact information (email, telephone) on the portal to ensure notifications are received. If you have an aggressive anti-spam filter, you should add the portal notifications to your "whitelist" or "safe senders". The email that you specify may be your work or your personal email, but beware that on a particularly active discussion topic, you may receive a dozen notification emails. Learn how to use email filters to prevent drowning in notifications. Regardless of email technical malfunctions, content posted online is an important part of this course and is incorporated as additional required readings unless otherwise specified.

Physical Attendance
Although we make use of online collaboration tools, this is not an "online course." Part of the pedagogy or learning process envisioned with this course is direct student-to-student discussion. This may take the form of online comment or debate on contemporary topics, blog postings, or news links. It also takes the form of physical in-class discussion and interaction. Unlike undergraduate studies, the instructor's purpose is not to lecture for three hours while students scribble down notes from the sage master. Rather, the instructor is an experienced tour guide, pointing out interesting sights (or "sites", pun intended) along the journey of cyber education.

Excused Absences
Your attendance and constructive participation in a corporeal fashion is an integral part of the successful completion of this course. However, there will be times when circumstances prohibit your attendance. Examples, in weighted order:

• Active or Reserve Duty military obligations
• Sickness, injury, physical disability
• Immovable business obligations
• Family obligations
• Transportation failures
• Vacation or Television marathons

In all cases, notification to the instructor prior to class is required. If your absence causes you to visit an interesting locale (e.g., State of the Union, toppling Mid-Eastern dictator's statue), consider sending a photo to share with our classroom community.

Readings Prior to Class
Students are required to complete reading assignments prior to the scheduled class meeting. If the label helps you, consider it "homework." The amount of reading assigned at a graduate level is certainly more than undergraduate studies. Successful students have been able to achieve near 100% comprehension without reading every printed word on the page. Nevertheless, what is expected is careful and thoughtful reading of the assigned texts. Truly engaged reading usually involves some form of notes, bookmarks, or highlighting. During the class, students will be expected to provide intelligent answers to questions posed and insightful commentary based on the assigned readings. Having a good resource of notes or bookmarks will assist you in providing this commentary for class discussion.

Seating Policy
This course meets in a large auditorium. As such, the instructor will provide guidance on seating to encourage class participation and eye contact with the instructor. A formal seating chart is not necessary, but limit the use of rows in the farthest half of the auditorium.

No Recording Policy
Audio and/or visual recording of any instructor, classmate, or guest lecturer is strictly forbidden, aside from disabilities that require the use of amplification or other recording devices. This course is intended to foster free discussion and recording devices produce a chilling effect on participation.

Special Needs Policy
Students with disabilities that need special accommodations should communicate these with the instructor and coordinate with SDSU Student Disability Services. If you have other non-disability related concerns or if you feel...
uncomfortable, overwhelmed, or unhappy, please communicate these to the instructor privately either after class or in email.

Non-Attribution Policy
This course (and the Homeland Security degree program) presents the student with a wide range of highly qualified and informative classmates, guest speakers, and instructors. To allow these individuals to speak candidly, they are assured that what is said in lecture, posted on the course website, or mentioned in other electronic, written, or verbal methods, will not be attributed to them outside the classroom, regardless of classification, disclaimer, or public domain. Quoting someone outside the course environment without permission risks calling fellow students, guest speakers, and instructors to account publicly for his or her opinions and comments. This most certainly would have the effect of stifling participation, causing them to speak in a guarded manner. Ultimately the quality of education provided would suffer. Hence, what your fellow students, guest speakers, and instructors say during their lectures is not for attribution. It may be acceptable to say "someone in my class" made a particular statement, but the individual's name will not be divulged. Individuals who violate this non-attribution policy are subject to adverse administrative and disciplinary action per University policy.

Non-Disclosure Policy
During certain presentations, discussions, or guest lectures, the instructors, guest lecturer, or fellow classmates may ask for discretion in a particular topic. The topic might not be for public distribution or the speaker is simply uncomfortable with its contents being discussed outside the classroom. In order to foster trust and open communication within our classroom, it is strictly required of anyone enrolled or involved in this course to maintain the secrecy of information properly identified as sensitive for a period of no less than five years or until such information enters the public domain or is otherwise released by its originator. Communication within class or on the course website is considered to be "not for disclosure" only if properly identified by the originator by explicit notification. For example, in an online posting that is not for disclosure, its originator should place a disclaimer before the text of a form similar to "NOT FOR DISCLOSURE". In verbal class discussions, a speaker can indicate a sensitive topic with a statement such as "the following should not leave this room" or similar admonition. Individuals who violate this non-disclosure policy are subject to adverse administrative and disciplinary action per University policy.

Government Security Clearance Policy
Some students, classmates, instructors, guest lecturers, or observers may be under the restrictions of certain U.S. Government Security Clearances issued by the Dept. of Defense, Dept. of Energy, Dept. of State, or other agencies. Those that hold these security levels must at all times remember their duty to uphold secrecy and must not at any time disclose any information that contradicts oaths, agreements, or pledges of secrecy that they have previously sworn or agreed to. At no point should there be a situation where a student mentions during a discussion "Well, this is classified information, but just don't tell anyone..." or similar situations. The previous non-disclosure policies will not protect someone that has knowingly violated their secrecy oaths and it is highly recommended that those with sensitive government clearances review the guidelines on information disclosure with their commanding officers and/or facility's information security officer.

For the protection of those that hold security clearances, please do not discuss or post online materials which you know or suspect to be under U.S. Government classification. Security clearances prohibit the handling or transmission of documents which exceed the classification level of the individual. While you may not be under such restrictions, your classmates might; your actions can have a detrimental effect on their ability to uphold their oaths, agreements, or pledges. CUI, SBU, U//FOUO, U//LES, and NOFORN are grey areas. When in doubt, please consult the instructor prior to discussion in class or online.

Anti-Plagiarism Policy
Confirmed plagiarism will result in a failing mark for the assignment and may result in more severe penalties including failure of the entire course and other University disciplinary methods. See Academic Policies on Cheating and Plagiarism for further guidance. By participating in this course, you acknowledge that the instructor may submit your written work to an online plagiarism detection system (such as TurnItIn.com) where it will be included in a reference database solely for the purpose of detecting plagiarism.

University Student Conduct Policies
Standards for Student Conduct (§41301, Title 5, California Code of Regulations) are published by the Student Affairs Office and apply to all courses at this university.