HSEC 690
Cyber Warfare & Cyber Terrorism

COURSE OVERVIEW

Intensive study in specific areas of homeland security with regards to nation-state cyber warfare. This course addresses the definition of, and challenges involved in "cyber warfare" as a subset of information warfare within the context of trans-national state-sponsored actors. To understand these concepts, this seminar will provide an overview of cyber-attack history, the difficulty with cyber-attribution, the myth of cyber-terrorism, the very real but poorly understood areas of cyber-espionage and cyber-sabotage. This course is not recommended for students from other disciplines interested purely in cyber security. **This course is not exhaustive, but it is intensive.** The purpose of this class is **NOT** to train the student in "how to hack computers." Students will learn the current state of cyber-attack, cyber-defense, and cyber-policy. Most importantly, the student will learn how to discern plausible cyber security threats from the improbable and hyperbolic.

PROGRAM LEARNING OUTCOMES

The mission of the Graduate Program in Homeland Security is to produce leaders from a variety of educational and professional backgrounds who can effectively and efficiently identify, design, and mobilize the appropriate community resources to identify, prevent, deter, preempt, defend against, and respond to terrorist attacks and/or other critical incidents and emergencies on the local, regional, national and international levels.

STUDENT LEARNING OUTCOMES

- ✓ Identify, analyze, synthesize, and disseminate information about threats and critical incidents.
- ✓ Demonstrate ability to appropriately use existing and develop new technology and scientific research to contribute to Homeland Security on a global basis.
- ✓ Articulate strategies for Homeland Security principles for the benefit our global partners.
- ✓ Identify important civil and human rights concerns generated by security needs and explain the appropriate balance of security with personal privacy, cybersecurity, and commerce.
- ✓ Demonstrate professional familiarity with US national standards and protocols (NIMS and ICS).
- ✓ Rapid sharing of information during disasters/events through social media interactions.
- ✓ Professional relationships with HSEC officials and businesses while securing borders and ports.
- ✓ Identify and delineate ethical issues related to HSEC including counter human trafficking.
- ✓ Interrelate the responses of the HSEC community to disasters of a natural origin such as fires, earthquakes, floods, tsunamis, and epidemics to the safety and wellbeing of the public.
- ✓ Accurate and responsible media communications in response to man-made and natural disasters.
- ✓ Improve HSEC solutions to address intersection of travelers, commerce, and international borders.

COURSE STRUCTURE

This course relies on various pedagogical approaches: reading assignments, instructor-guided discussions, student briefings, and projects. Reading assignments are an important self-learning tool and the classroom discussion is designed to supplement the reading by clarifying and elaborating concepts. As a seminar course, the instructor will rely on students to participate actively in discussion and critical thinking. Students should not hesitate to question and discuss controversial topics in an open and non-judgmental educational environment.

REQUIRED COURSE MATERIALS

Required course materials and grading categories are posted online at: **homelandsecurity.sdsu.edu/cyber**

COURSE POLICIES

By participating in this course, you acknowledge and accept the policies herewith and will e-sign at: **sign.sdsu.edu/hsec/policies**