Figure 1. CYSE 200T Course Syllabus Screenshot.

Source: Old Dominion University (n.d.). Canvas course page. https://canvas.odu.edu/courses/201814

IT/CYSE 200T

Cybersecurity, Technology, and Society

CYSE 200T – Course Overview & Description

Course Description

Students explore how technology relates to cybersecurity from an interdisciplinary perspective. Attention is given to how technologically driven cybersecurity issues are connected to cultural, political, legal, ethical, and business domains.

Specifically, the exploration of how the disciplines of business, technology, criminal justice, sociology, psychology, and philosophy contribute to cybersecurity.

The Big Question

Working through assignments and the other aspects of this course, remember the following "Big Question."

What are the interdisciplinary intersections, emerging trends, and issues in the field of cybersecurity?

Exit skills

Upon completion of this course, students will be able to...

1. Describe how cyber technology creates opportunities for criminal behavior.
2. Identify how cultural beliefs interact with technology to impact cybersecurity strategies.
3. Understand and describe how the components, mechanisms, and functions of cyber systems give rise to security concerns.
4. Discuss the impact of cyber technology on individuals' experiences of crime and victimization.
5. Understand and describe both intended and unintended ethical dilemmas that cybersecurity efforts produce for individuals, nations, societies, and the environment.
6. Describe the costs and benefits of producing secure cyber technologies.
7. Understand and describe the global nature of cybersecurity and the way that cybersecurity efforts have produced and inhibited global changes.
8. Describe the role of cybersecurity in defining appropriate and inappropriate behavior.
9. Describe how cybersecurity produces ideas of progress and modernism.

CYSE-200T focuses on cybersecurity through multiple disciplinary lenses, comprising seven distinct modules. The core aim is to explore cybersecurity issues that are technologically driven yet connected to broader cultural, political, legal, ethical, and business domains.

Weekly Course Outline

Week 1

Module 1: Intros, Definitions & History: This module introduces the multi- vs. transdisciplinary nature of cybersecurity, basic definitions, the roles of various disciplines, and security frameworks. Learning objectives include discussing key historical events and developing an understanding of the makeup of an "IT System" beyond just technology.

Weeks 2 - 6

Module 2: Cybersecurity in Business: This module covers fundamental business concepts, including Operations, Finance, Marketing, Sales, IT, and Human Resources, and how Information Technology and Cybersecurity support these functions. It also explores Risk Management and Business Writing Skills, focusing on the concepts of and relationships between vulnerabilities, threats, exposures, and countermeasures.

Week 7

Module 3: IT & BioCyber: This module focuses on an introduction to the Biological Sciences Industry, potential unique vulnerabilities in this field, and associated ethical considerations. Key topics include relating advances in biological research (e.g., CRISPR/Cas9 gene editing) to subsequent sections on philosophy and ethics and discussing potential privacy concerns arising from these advancements. (CRISPR stands for Clustered Regularly Interspaced Short Palindromic Repeats, and Cas9 stands for CRISPR-associated protein 9)

Weeks 8 - 9

Module 4: Computer Science: Module 4 explores foundational technical concepts, including authentication, Authorization, Encryption Techniques, Attack Vectors, and Countermeasures. Objectives include explaining hashing mechanisms, exploring security terminology, and covering mechanisms such as firewalls and Virtual Private Networks (VPNs) used to protect systems.

Weeks 10 -11

Module 5: Engineering & Critical Infrastructure: This module discusses the impact of cyber technology and attacks on engineering systems, identifies common vulnerabilities in these systems, and describes fundamental design principles for resilience. It explicitly introduces Supervisory Control & Data Acquisition (SCADA) systems, which are used to manage critical infrastructure such as energy, agriculture, and transportation.

Weeks 12 - 13

Module 6: Criminal Justice & Cybersecurity: The module examines the intersection of Criminal Justice and Cybersecurity, covering different types of cybercrime, the evolution of criminal justice with cyber technology, and shifting definitions of right and wrong. Topics addressed include cyber harassment, cyber stalking, and the challenges cybercrime poses to the justice system.

Weeks 14 - 15

Module 7: Philosophy Aspects of Cybersecurity: This final module addresses the philosophical aspects of cybersecurity, focusing on questions like what is "Good/Bad for Society," societal responsibilities, and individual responsibilities. It examines ethical dilemmas, such as balancing business obligations with professional obligations to the public good, and the societal impact of technology.

Note: Course overview and module descriptions adapted from Old Dominion University (n.d.), *Cybersecurity, Technology, and Society, CYSE 200T syllabus materials.*