

ENF665 Cyber Security and Technology in Homeland Security (3 credit hours) Course Syllabus

Course Description

This course examines the impact of cyber and technology on the Homeland Security Enterprise. Students will analyze laws, policies, and other governance structures for cybersecurity and technology. Students will review past, current and future technology typologies and deployments within the Homeland Security Enterprise. An examination of the cyber threat environment and cyber terrorism through a risk assessment and management process will allow students to quantify and mitigate cyber risk. The course analyzes past, current, and future trends in data management, including interoperable communication systems, information sharing initiatives and technologies, and standards and their importance to the Homeland Security Enterprise. Finally, an examination of the interdependencies of technology and cyber systems as they relate to critical infrastructure.

Course Learning Outcomes

By the end of this course, you will be able to:

1. Critique U.S. cybersecurity policy as it relates to the Homeland Security Enterprise.
2. Identify and analyze cyber threat vectors.
3. Evaluate interoperable communication and information sharing systems.
4. Apply and evaluate risk assessment techniques to quantify risk.
5. Plan and justify risk mitigation strategies.
6. Categorize and assess current and emerging technologies within the Homeland Security Enterprise.

Required Textbook(s) and Resources

A printed copy of your textbook is included with your DragonACCESS fees for this course. The book will be shipped from the Tiffin bookstore approximately 2 weeks before the start of classes.

Buchanan, Ben. 2020. *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. Cambridge: Harvard University Press.

Be sure to also review the weekly **Explore** sections for additional library or web resources. For access to databases, research help, and writing tips, visit the [Tiffin University Library](#). You might consider registering for one of the library's many webinars on library research, source evaluation, copyright, and other topics, at the [Library Events - Upcoming Events](#) web page. For further assistance email a librarian, at: library@tiffin.edu.

Time Commitment

Effective time management is possibly the single most critical element to your academic success. To do well in this online class you should plan your time wisely to maximize your learning through the completion of readings, discussions, and assignments. Because of our accelerated, seven-week term, TU online courses are designed with the expectation that you dedicate a little over **six (6)** hours per credit hour to course activities and preparation **each week**. For example, for successful completion of a three-credit, seven-week online course you should reserve roughly **twenty (20) hours per week**.

To help plan your time and keep on track toward successful course completion, note the distinctive rhythm of assignment due dates:

1. All times assume Eastern Time (GMT-4).
2. Weeks begin at 12:00 a.m. ET on Monday and end at 11:55 p.m. ET on Sunday.
3. Unless otherwise noted, initial assignments or discussion posts are due by **11:55 p.m. ET on Wednesdays**.
4. Additional assignments or follow-up discussion posts are due by **11:55 p.m. ET on Saturdays, and**
5. Major assignments and reflections are typically due by **11:55 p.m. ET on Sundays**.

Learning Activities

During this course students will experience the value of peer-to-peer learning through weekly discussion forums and papers in which you will critique the current state of cybersecurity, examine the collaborative efforts by public and private sectors to safeguard US information, networks, and data, explain common threat vectors used by cyber actors to target US networks, identify best practices for interoperable communication within the Department of

Homeland Security, and develop a cyber-centric risk analysis for critical infrastructure, industrial control systems (ICSs) and supervisory control and data acquisition (SCADA) systems. Students will also complete one presentation during week 7 that includes developing a risk mitigation strategy for a tabletop exercise scenario with real-world implications.

Grading

The chart below identifies the individual contributions from each type of activity, per week.

Week 1	Week 2	Week 3	Week 4	Week 5	Week 6	Week 7	Total
Discussions Activity 1.1 (0) Activity 1.2 (40)	Discussions Activity 2.1 (40)	Discussions Activity 3.1 (40)	Discussions Activity 4.1 (40)	Discussions Activity 5.1 (40)	Discussions Activity 6.1 (40)	Discussions Activity 7.1 (40)	280
Assignments Activity 1.3 (100)	Assignments Activity 2.2 (100)	Assignments Activity 3.2 (100)	Assignments Activity 4.2 (100)	Assignments Activity 5.2 (100)	Assignments Activity 6.2 (100)		600
						Presentation Activity 7.2 (120)	120
140	140	140	140	140	140	160	1000

Grading Scale

Grade	Percentage
A	90-100%
B	80-89%
C	70-79%
F	<70

Please see the [Academic Bulletin](#) for grade appeal information.

Course Schedule and Weekly Checklist

Topic	Learning Activities (Due by 11:55 p.m. ET on day designated)
Start Here	<input type="checkbox"/> MON: Activity 1.1: Hello! Please Introduce Yourself!
Week 1: DHS Cybersecurity Strategy Current cybersecurity threats to the Homeland Security Enterprise	<input type="checkbox"/> WED: Activity 1.1: Hello! Please Introduce Yourself! - Secondary Post <input type="checkbox"/> WED: Activity 1.2: Critiquing the Current State of U.S. Cybersecurity <input type="checkbox"/> SAT: Activity 1.2: Critiquing the Current State of U.S. Cybersecurity <input type="checkbox"/> SUN: Activity 1.3: How IoT Devices can Impact Homeland Security
Week 2: NIST Cybersecurity Framework National Infrastructure Protection Plan CISA's Global Initiative	<input type="checkbox"/> WED: Activity 2.1: The Role of Government & The Private Sector in Managing Risks <input type="checkbox"/> SAT: Activity 2.1: The Role of Government & The Private Sector in Managing Risks <input type="checkbox"/> SUN: Activity 2.2: CISA Initiatives to Improve the Cybersecurity Ecosystem
Week 3: Cyber threat actors Cyber threat vectors US Critical Infrastructure	<input type="checkbox"/> WED: Activity 3.1: Examining Common Threat Vectors <input type="checkbox"/> SAT: Activity 3.1: Examining Common Threat Vectors <input type="checkbox"/> SUN: Activity 3.2: Securing Critical Infrastructure
Week 4: NIMS Communication and Information Management	<input type="checkbox"/> WED: Activity 4.1: Developing an Interoperable Communications Plan <input type="checkbox"/> SAT: Activity 4.1: Developing an Interoperable Communications Plan <input type="checkbox"/> SUN: Activity 4.2: Overcoming Challenges in the National Emergency Communications Plans

National Emergency Communications Plan Homeland Security Information Network	
Week 5: THIRA Risk Assessment Risk Matrix Template Cyber Vulnerabilities ICS/SCADA	<input type="checkbox"/> WED: Activity 5.1: Strengths & Weaknesses of Risk Assessments <input type="checkbox"/> SAT: Activity 5.1: Strengths & Weaknesses of Risk Assessments <input type="checkbox"/> SUN: Activity 5.2: Analyzing & Assessing ICS/SCADA Risks
Week 6: Supply Chain Risk Management IoT Vulnerabilities Critical Infrastructure	<input type="checkbox"/> WED: Activity 6.1: Examining Plausible Future Crises <input type="checkbox"/> SAT: Activity 6.1: Examining Plausible Future Crises <input type="checkbox"/> SUN: Activity 6.2: Evaluating Global Impacts of Supply Chain Attacks
Week 7: 5G Integration Artificial Intelligence IoT devices	<input type="checkbox"/> WED: Activity 7.1: Planning a Cyber Attack Scenario <input type="checkbox"/> FRI: Activity 7.1: Planning a Cyber Attack Scenario <input type="checkbox"/> SUN: Activity 7.2: Final Project - The Future is Plural: Mitigating Risks

Tips for Success

Successful online learning requires a good deal of self-discipline and self-direction. As seekers of the truth, we should be willing to challenge and review one another's academic work in a spirit of respectful comradery and constructiveness. Your course is a place for you to stretch and grow as you benefit from the expertise, knowledge, experience and diverse perspectives of your instructor and peers. Constructive feedback will challenge you to stretch your own thinking, thereby expanding your knowledge, understanding and application.

To get the most out of your learning experience, you should actively engage (participate) in **ALL** course activities. Course elements are arranged chronologically. To complete a week, simply work your way "down the page" through all of the course materials and activities.

Your Instructor Will Expect You to:

- Thoroughly review orientation materials (Start Here) within the first 48 hours of the term.
- Monitor your TU email account **daily** for important updates and announcements.
- Take ownership of your learning experience and act in a proactive, self-directed manner. That means:
 - Fully participate in all learning activities.
 - Complete assignments as described in rubrics or other instructions.
 - Submit all work on time and in the specified format (e.g. APA format for citations). Late assignments will be accepted at the discretion of your instructor. Penalties may apply.
 - Utilize and incorporate instructor provided feedback to improve your work.
 - Ask questions so you can better understand course material or assignments.
 - Use the highest standards of intellectual honesty and integrity. For more information, see the TU Library guide: [Digital Literacy: Netiquette and Internet Safety](#).
 - Treat others respectfully and demonstrate "netiquette" (online politeness and respectfulness) at all times. TU celebrates cultural uniqueness and expects all students to be considerate and thoughtful throughout their learning experiences.

You Should Expect Your Instructors to:

- Post an introductory announcement/email at the beginning of each week to provide updates and help you prepare for the week's activities.
- Maintain an active and engaged presence in all course activities and throughout the course.
- Respond to your emailed questions within 48 hours, if not sooner.
- Clearly communicate any absences or expected non-participation due to extenuating circumstances. For example, "I will be traveling to attend a funeral this week and may not be able to respond to questions or participate in forums for a couple of days."
- When grading your work:
 - clearly indicate their grading approach (what they like to see in submitted work as well as what types of errors they tend to penalize more harshly),
 - thoroughly review and evaluate your submissions in a timely manner (in less than 5 days for most assignments), and

- provide constructive feedback that indicates the strengths and weaknesses of your work and provides suggestions on how you can improve your performance on future assignments.
- Advocate for your success as a learner and help guide you toward successful completion of the course activities and most importantly, attainment of the course learning outcomes.

Accommodations

The **Office for Disability Services** supports the institutional commitment to diversity by providing educational opportunities for qualified individuals with disabilities through accessible programs and services in compliance with Section 504 of the Rehabilitation Act of 1973 and Title III of the Americans with Disabilities Act (ADA) of 1990.

If you need reasonable accommodations due to a documented disability, contact the Office for Equity, Access, & Opportunity 419.448.3021 or via email at disabilityservices@tiffin.edu.

Additional Resources & Support

For technical support, either email moodlesupport@tiffin.edu or call the 24/7 Technical Support Call Center at 855-664-1200.

If you need to consult an academic advisor refer to TU's [Meet the Team](#) page.

For information about TU's peer tutoring program see the Murphy Center's [Tutoring Policies and Procedures](#) page. Veterans and active military can seek assistance from TU's [Veteran and Military Services Web Page](#).

Comments or Concerns

TU's online programs are designed to be student-driven: to empower you with a voice and stake in your learning. Our courses feature multiple and varied ways that you can share feedback, and we invite you to become an active voice and help drive our improvement efforts. In addition to providing in-course feedback, we encourage you to submit questions or comments directly to the online team at online@tiffin.edu.