

# COMP-4733 Course Syllabus

## 1 Course Information

Course Name	COMP 4733: Artificial Intelligence for Cybersecurity
Prerequisites	COMP-4006
Required Textbook	No textbook required

## 2 Course Description

This course provides an accessible introduction to artificial intelligence and machine learning with a focus on applications in cybersecurity. Designed for students with a wide range of backgrounds, including those with little to no prior experience in AI, the course emphasizes practical skills and real-world relevance. Over a 10-week period, students learn foundational AI and ML concepts and apply them to contemporary cybersecurity challenges.

The structure of the course is heavily project-based, culminating in a substantial final project completed individually or in groups. Throughout the term, students develop solutions to realistic security problems such as detecting malicious activity in network traffic, classifying benign versus malicious behavior, and analyzing system vulnerabilities using AI-driven techniques. The concentrated focus on cybersecurity applications supports strong student engagement and encourages exploration beyond the minimum requirements, including experimentation with multiple models, performance optimization, and use of diverse datasets.

The course aims to equip students with practical, industry-aligned skills at the intersection of two rapidly evolving fields: artificial intelligence and cybersecurity. Students complete the course with hands-on experience, portfolio-ready projects, and exposure to tools and methods that reflect current trends in the cybersecurity landscape.

## 3 Textbook and Materials

There is no required textbook for this course. Textbooks for the concepts covered in this class generally do not evolve as quickly as the technology.

Textbook recommendations for each time the course is offered may be made in Canvas.

You will need a good internet connection and a laptop that meets DU specifications. (See <https://www.du.edu/it/support/how-to/students/laptops>). For technical support in using Canvas, please go to <http://otl.du.edu/knowledgebase/canvas>

## 4 Course Topics

1. Foundations of Artificial Intelligence and Machine Learning
2. History, ethics, and societal impacts of AI
3. Search and optimization algorithms
  - (a) Depth-First Search (DFS), Breadth-First Search (BFS), A\* and heuristic search, Minimax and alpha-beta pruning
4. Knowledge representation and reasoning
  - (a) Propositional and first-order logic, Model checking and logical inference
5. Probabilistic reasoning and uncertainty modeling
  - (a) Bayesian networks, Markov models
6. Reinforcement learning
  - (a) Q-learning and policy optimization, Sequential decision-making and reward systems
7. Supervised and unsupervised learning
  - (a) Classification, regression, and clustering, Model evaluation and performance metrics
8. Neural networks and deep learning
  - (a) Feed-forward, convolutional, and recurrent architectures, Backpropagation and gradient descent, Transfer learning and fine-tuning
9. Natural Language Processing (NLP)
  - (a) Formal grammars and statistical language models, Transformer architectures and attention mechanisms, Large Language Models (LLMs) and Retrieval-Augmented Generation (RAG)
10. AI for cybersecurity
  - (a) Anomaly, intrusion, and fraud detection, Adversarial attacks and AI system vulnerabilities, AI model robustness, interpretability, and security, AI-powered cyber defense and automation tools
11. Data science for threat intelligence
  - (a) Pattern and anomaly detection in threat data, Predictive analytics for security monitoring

12. Digital forensics and AI applications
  - (a) Evidence extraction, correlation, and analysis, Use of AI in forensic automation and investigation workflows
13. Secure and ethical AI deployment
  - (a) Responsible AI principles, Data privacy, bias mitigation, and system accountability

## 5 Course Learning Outcomes

The high level learning outcomes of this course are as follows:

- Build, train, and evaluate machine learning models.
- Apply AI and ML techniques to cybersecurity problems such as phishing detection, anomaly detection, and intrusion analysis.
- Work with real-world datasets and industry-relevant tools used in security analytics and cyber defense.
- Analyze network or system data to detect and classify malicious activity using AI/ML approaches.
- Develop and present a substantial project demonstrating applied AI methods for solving cybersecurity challenges.

## 6 Program Level Goals

Courses in the cyber security MS program, including this one, should contribute to overall program level outcomes for students. This course contributes to the following program level goals:

1. **Be familiar with modern AI frameworks, models and tools and how they relate to or can be leveraged in Cybersecurity contexts.**
2. **Understand common cyber security vocabulary, and understand and intelligently discuss cyber security topics (incidents, advisories, etc.)**
3. **Apply programming and core CS topics; including network programming, algorithms and data structures, and computer organization.**

## 7 Knowledge Units

This course covers the following NSA cybersecurity Knowledge Units:

1. IT Systems Components (ISC, Foundational CDE)
2. Network Defense (NDF, Core Technical CDE)
3. Systems Programming (SPG, Optional KU)

## 8 Attendance Policy

Regular attendance is expected. Students are responsible for all material covered in class, including announcements and handouts.

## 9 Academic Integrity

All work submitted for this course must be the student's own original work. Any instance of plagiarism or cheating will be dealt with according to the university's academic integrity policy. Refer to the Student Rights and Responsibilities, as well as the University of Denver Student Honor code, here: <https://studentaffairs.du.edu/student-rights-responsibilities>

## 10 Disability Services

If you have a disability that may affect your ability to complete the work for this course, please contact the Disability Services office at: <https://studentaffairs.du.edu/disability-services-progr>