國立東華大學

課　　綱　Course Outline

理工學院碩士班

中文課程名稱 Course Name in Chinese	大型語言模型與資訊安全系統				
英文課程名稱 Course Name in English	Applying Large Language Models in Cybersecurity Systems				
科目代碼 Course Code	TCAI50110	班 別 Degree	碩士班 Master’s		
修別 Type	選修 Elective	學分數 Credit(s)	3.0	時 數 Hour(s)	3.0
先修課程 Prerequisite					

課程目標
Course Objectives

課程大綱
Course Outline

Can AI cyber defend with us?
This opening theme sets the stage by asking whether AI can act as a partner in defending cyberspace. We will examine how AI shifts
from a passive tool to an active collaborator.

AI Evolution, a cybersecurity focus
We trace the evolution of AI, with emphasis on how each wave—from expert systems to LLMs—intersects with security.

True AI+ Cybersecurity Stories
Real-world case studies illustrate how AI has already been used in cyber defense and offense.
We will examine success stories, failures, and lessons learned.

AI & Cybersecurity Lingo
This module builds a shared vocabulary at the intersection of AI and security.
Students learn terms used in both communities to prevent
miscommunication.

Prompting AI for Cybersecurity
Students learn how to craft effective prompts for LLMs in security tasks. We discuss prompt design, adversarial prompting, and failure cases.

Data Curation for Cybersecurity
We explore how security data must be cleaned, structured, and curated for effective AI use.
Students will learn challenges of logs, alerts, and threat intelligence feeds.

Machine Learning for Cybersecurity
This module covers classical and modern machine learning applied to intrusion detection, anomaly detection, and malware classification.
Students will see how supervised, unsupervised, and reinforcement learning differ in security contexts.

Developing AI-powered Cyber Defense
We transition from theory to system building. Students design end-to-end workflows for AI-driven defense, including data pipelines,
model integration, and automation layers.

Governing Ethics and Security
AI in security raises governance and ethical concerns. Students study bias, accountability, explainability, and dual-use risks. We also cover standards, regulations, and compliance frameworks.

True AI+ Cybersecurity Stories
A second set of case studies builds on earlier discussions, with deeper analysis of emerging trends. We examine ongoing incidents where AI is suspected to play a role.

AI for Cybersecurity
We focus on how AI enhances security functions such as monitoring, detection, and response. Students review tools and frameworks
that integrate AI in SOC workflows.

Cybersecurity for AI
Here the perspective flips: securing AI systems themselves. Students examine threats to models, data pipelines, and APIs. Topics include
adversarial attacks, data poisoning, and model theft.

PBL: AI+ Security Requirements
Teams begin project-based learning by gathering requirements for an AI+security solution. The focus is on defining scope, use cases, and
constraints.

PBL: AI+ Security Design
Teams progress to high-level and detailed design. Students create system architectures, data flows, and defense logic. Emphasis is on
aligning design with requirements while considering risks.

PBL: AI+ Security POC
Teams implement a proof-of-concept based on their designs. The emphasis is on demonstrating feasibility, not completeness. Students test core functions and identify limitations.

PBL: AI+ Security Solution
The course culminates with a full solution built from requirements, design, and POC iterations. Students deliver a working system or detailed prototype.

資源需求評估（師資專長之聘任、儀器設備的配合・・・等）
Resources Required (e.g. qualifications and expertise, instrument and equipment, etc.)

課程要求和教學方式之建議

Course Requirements and Suggested Teaching Methods
其他 Miscellaneous