主導課程：大型語言模型與資訊安全系統（Applying Large Language Models in Cybersecurity Systems）

課程基本資料

開設學校：國立台灣科技大學

開授教師：林俊叡

班級人數：聯盟學校每校上限100人

開課級別：研究所

授課語言：英文

授權方式：封閉型

協同教師學經歷建議：

同步遠距上課時間：

- 台科大上課時間：週一 9:20–12:20，第一個小時為線上課程自修；10:20–12:20 為直播演練時間。
- 聯盟學校學生可非同步上課，先自行完成一小時線上自修，其餘兩小時則於助教固定時段（週一至週五擇一時段，未來將補充公布）參與線上練習，此練習為必修環節，所有學生皆須參與。

是否也接受非同步授課：是

實體評量時間：沒有考試，但是週週有作業，週週給作業評分

遠距上課位置：TBD

課程網頁：TBD

建議聯盟學校修課人數與助教比例：由於作業繁多，建議每20名學生需1名助教

課程概述

本課程探討大型語言模型（LLMs）如何重塑資安領域。學生將學習如何運用 AI 於安全任務、資料整理、機器學習與防禦系統開發。透過專題式學習，團隊將設計並測試真實的 AI+資安解決方案，同時思考倫理、治理，以及「保護 AI」與「運用 AI 防禦」的雙重挑戰。

Applying Large Language Models in Cybersecurity Systems introduces students to the rapidly evolving intersection of artificial intelligence and cyber defense. The course explores how large language models (LLMs) are transforming cybersecurity practice, from automated threat detection to intelligent defense solutions, while also addressing the unique security challenges AI itself introduces.

Students will begin by examining the question “Can AI defend with us?”—a guiding theme that frames the role of AI as both an ally and a potential risk in digital security. The course then surveys the evolution of AI with a cybersecurity focus, real-world case studies, and the key terminology that shapes the field.

Practical skills are emphasized through modules on effective prompting, data curation for threat intelligence, and applying machine learning techniques to security problems. Students will gain hands-on experience in designing, developing, and evaluating AI-powered cyber defense systems, while also considering governance, ethics, and security implications.

A distinctive feature of the course is its Project-Based Learning (PBL) track, where students work in teams to translate theoretical knowledge into practical solutions. Through progressive milestones—requirements, design, proof-of-concept, and final solution—students will learn how to build and evaluate AI-driven security applications that can operate in real-world environments.

By the end of the course, students will be equipped not only with technical competencies in AI and cybersecurity integration but also with the critical perspective required to navigate ethical, organizational, and security governance challenges.

指定書目

Think Artificial Intelligence: A Student’s Guide to AI’s Building Blocks, by Jerry Cuomo

參考書目

Practical AI for Cybersecurity, by Ravi Das

ChatGPT for Cybersecurity Cookbook: Learn Practical Generative AI Recipes to Supercharge Your Cybersecurity Skills, by Clint Bodungen

課程大綱

週次	日期	課程主題	課程內容	備註
1	2/23	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.	
2	3/2	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.	
3	3/9	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.	

4	3/16	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.	
5	3/23	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.	校慶放假一日，當週仍有進度。
6	3/30	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.	
7	4/6	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.	清明連假放假一次，當週仍有進度。
8	4/13	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.	
9	4/20	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.	
10	4/27	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.	
11	5/4	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.	
12	5/11	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.	
13	5/18	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.	
14	5/25	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.	
15	6/1	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.	
16	6/8	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.	

成績評量方式

- Weekly assignments are graded on a scale of **1–5 points** (0 if not submitted).
- The **total score** is calculated as **20 base points + the sum of all assignment points**, with a maximum of **100 points**.