國立台灣科技大學 114學年 第2學期　課程大綱

Spring 2026 NTUST Course Outline

授課教師：林俊叡

Instructor:Raymund Lin

課程名稱：大型語言模型與資訊安全系統

Course Title：Applying Large Language Models in Cybersecurity Systems

2026/11/3

課程代號： MI5137701 Course Code 學分數： 3 Credits	必選修：選修/半學年 Required/Electve:Elective/Half Yr. 先修課程： Prerequisites
節次教室： Time/Location	M3(MA-303) M4(MA-303) M5(MA-303)
專業核心能力： Core Professional Competencies	■解決問題之能力(Problem Solving) ■創新與創業能力(Innovation and Entrepreneurship)
課程網址： Course Website	https://taicatw.net/spring-114/
課程宗旨： Course Objectives	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.
課程大綱： Outline of Lectures	

Course Topics (English)

1. Can AI Cyber Defend with Us?
2. AI Evolution with a Cybersecurity Focus
3. AI + Cybersecurity Case Studies (I)
4. AI & Cybersecurity Terminology
5. Prompting AI for Cybersecurity
6. Data Curation for Cybersecurity
7. Machine Learning for Cybersecurity
8. Developing AI-Powered Cyber Defense Systems
9. Governance, Ethics, and Security in AI
10. AI + Cybersecurity Case Studies (II)
11. AI for Cybersecurity Operations
12. Cybersecurity for AI Systems
13. PBL: AI + Security Requirements Analysis
14. PBL: AI + Security System Design
15. PBL: AI + Security Proof of Concept (PoC)
16. PBL: AI + Security Integrated Solution

課程主題（繁體中文）

1. AI 能否與我們共同進行網路防禦？
2. 人工智慧的演進：以資安為核心視角
3. AI 與網路安全實務案例（一）
4. AI 與網路安全專業術語
5. 資安應用中的 AI 提示工程
6. 網路安全資料整理與治理
7. 網路安全中的機器學習方法
8. AI 驅動之網路防禦系統開發
9. AI 的治理、倫理與安全議題
10. AI 與網路安全實務案例（二）
11. AI 在網路安全營運中的應用
12. AI 系統本身的網路安全
13. 專題導向學習：AI＋資安需求分析
14. 專題導向學習：AI＋資安系統設計
15. 專題導向學習：AI＋資安概念驗證（PoC）
16. 專題導向學習：AI＋資安整合解決方案

授課方式： Method of Instruction	講授 Lecture：30% 分組討論 Group discussion：10% 案例研討 Case study：10% 操做練習 Practical exercises：50% 講授 Lecture：There are no exams in this course; however, students will complete weekly workshops and assignments. Please refer to the grading section for details on how assignment outcomes contribute to the final grade.%
教科書： Textbooks	Think Artificial Intelligence: A Student’s Guide to AI’s Building Blocks, by Jerry Cuomo
參考書目： References	Practical AI for Cybersecurity, by Ravi Das ChatGPT for Cybersecurity Cookbook: Learn Practical Generative AI Recipes to Supercharge Your Cybersecurity Skills, by Clint Bodungen
修課須知： Notice	This course is now part of the TAICA initiative. For students wishing to get TAICA certificates, please consult: https://taicatw.net/
評量方式： Grading	● 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.
備註說明： Notes	Students wishing to enroll in this course are advised to possess foundational knowledge in both Artificial Intelligence and Cybersecurity.