

Welcome & Administrative Matters

MSCS 640: Artificial Intelligence and Cyber Security

Dr. Mouatez Karbab



أكاديمية جوعان بن جاسم للدراسات الدفاعية
Joaan Bin Jassim Academy for Defence Studies

September 7, 2026



Outline

- 1 Course
- 2 Learning Materials
- 3 Methodology



Outline

- 1 Course
- 2 Learning Materials
- 3 Methodology



Course Information

Course:	Artificial Intelligence and Cyber Security
Code:	MSCS 640
Program:	Master of Science in Cyber Defense
Type:	Compulsory
Credit:	3
Hours:	Mondays 17:00-20:00
Room:	Lab Room
Webpage:	https://courses.karbab.net/mscs640/
Instructor:	Dr. ElMouatez Billah Karbab
Email:	mouatez@karbab.net



Outline

- 1 Course
- 2 Learning Materials
- 3 Methodology



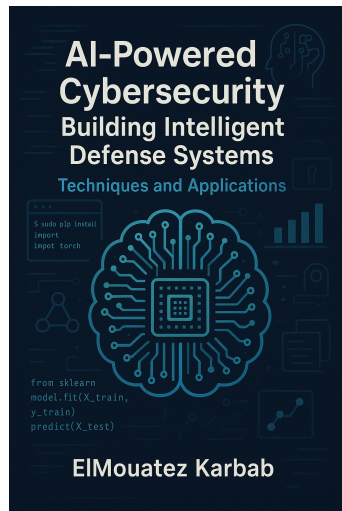
Learning Materials

- **Mandatory Textbook:** AI-Powered Cybersecurity: Building Intelligent Defense Systems, Techniques and Applications ElMouatez Karbab (2026) (<https://books.karbab.net/ai-cybersec/>)
- **Optional:** Parisi, A. (2019). Hands-On Artificial Intelligence for Cybersecurity: Implement smart AI systems for preventing cyber attacks and detecting threats and network anomalies. Packt Publishing Ltd.
- **Optional:** Halder, S., & Ozdemir, S. (2018). Hands-On Machine Learning for Cybersecurity: Safeguard your system by making your machines intelligent using the Python ecosystem. Packt Publishing Ltd.



Learning Materials

Mandatory Textbook: AI-Powered Cybersecurity: Building Intelligent Defense Systems, Techniques and Applications ElMouatez Karbab (2026) (<https://books.karbab.net/ai-cybersec/>)



Outline

- 1 Course
- 2 Learning Materials
- 3 Methodology



Methodology

- Activities Process
- Educational Process
 - ① **Learner Engagement**
 - ② **Violation of intellectual and moral rights**
 - ③ **Cases of late delivery or non-delivery of duties**
 - ④ **Conduct**

Assessment and Grading

Assessment Tool	Timing	Grade
Participation	During The Semester	15
Labs	During The Semester	15
Project	Submission on Week 12	30
Final Exam	Week 15	40
Total		100



Course Schedule I

This schedule is tentative and subject to change at the instructor's discretion.

Week	Topic	Readings
Week 1	Foundations of AI-Driven Cybersecurity Lab: Python for ML and Data analytics	Chapter 1
Week 2	ML Essentials for Cybersecurity, Phishing Email Detector Lab: End-to-End Phishing Email Detector	Chapter 3 Chapter 4
Week 3	ML based Network Intrusion Detection Lab: End-to-End Network Intrusion Detection	Chapter 5 Chapter 6
Week 4	Deep Learning for Malware Analysis Lab: End-to-End malware Detection Final Project Proposal Due	Chapter 7
Week 5	AI for In-Vehicle Network Security Lab: CAN Bus Intrusion Detection	Chapter 8
Week 6	AI for Sensor Security in CPS Lab: Sensor Integrity in CPS	Chapter 9



Course Schedule II

Week 7	Transformers for Advanced Security NLP Lab: Detecting Malicious Emails with Transformers	Chapter 10
Week 8	Sequence Models for Temporal Anomaly Detection Lab: Detecting Impossible Travel	Chapter 11
Week 9	Unsupervised Methods for Zero-Day Detection Lab: Zero-Day & Novel Attack Detection	Chapter 12
Week 10	Graph Neural Networks for Relationship Analysis Lab: GNNs for Cybersecurity Threat Detection	Chapter 13
Week 11	MLOps in Cybersecurity Lab: MLOps, Intrusion Detection	Chapter 15
Week 12	Model Evaluation & Continuous Validation Lab: Model Evaluation & Drift Detection in the SOC	Chapter 16
Week 13	Privacy, Ethics, and Governance in AI Lab: Building a Fair and Privacy-Aware NIDS Final Project Due	Chapter 17
Week 14	Future Directions & Advanced Topics Lab: Adversarial ML in Cybersecurity	Chapter 18
Week 15	Final Exam	

Thank You!

