



Artificial Intelligence and Cyber Security

MSCS 640 - Fall 2026

COURSE

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

COURSE DESCRIPTION

This course provides a rigorous and practice-oriented examination of the design, development, and deployment of intelligent artificial intelligence (AI) solutions tailored to address pressing challenges in modern cybersecurity [2]. It is structured to equip students with both the theoretical foundations and the applied technical skills necessary to conceptualize, implement, and operationalize AI-driven defensive systems within complex and dynamic security environments.

The curriculum begins with a systematic introduction to foundational principles, ensuring that students gain a clear and structured understanding of key concepts in AI and cybersecurity. The course scaffolds learning by progressively building from basic definitions to advanced methodologies. Throughout the course, Python serves as the primary programming language, supplemented by widely adopted machine learning and deep learning libraries. This approach allows students to gain hands-on experience in implementing state-of-the-art algorithms and techniques for a diverse range of security applications, including phishing detection, network intrusion analysis, anomaly detection, and malware classification [1, 3].

Beyond technical implementation, the course emphasizes the broader operational and organizational dimensions of deploying AI in cybersecurity contexts. Students will engage with topics such as machine learning operations (MLOps), lifecycle management of AI models, and the necessity of continuous validation in adversarial and rapidly evolving threat landscapes [4]. Furthermore, the course addresses ethical, legal, and governance considerations, encouraging students to critically reflect on issues such as algorithmic fairness, transparency, accountability, and the societal impact of AI-enabled security systems [5].

By integrating theoretical insight, technical skill development, and critical reflection, this course aims to prepare students to contribute meaningfully to the emerging field of AI-driven cybersecurity, whether in research, industry, or policy-making contexts.

OBJECTIVES

Upon successful completion of this course, students will be able to:

- Demonstrate a foundational understanding of key concepts in artificial intelligence (AI) and cybersecurity, and explain their interrelationships.
- Design, train, and evaluate AI models for tasks such as phishing detection, network intrusion analysis, anomaly detection, and malware classification.
- Apply Python programming and widely used machine learning/deep learning libraries to implement AI-based solutions for cybersecurity challenges.
- Critically assess the operational requirements of deploying AI in real-world security systems, including model lifecycle management, continuous validation, and adaptability to evolving threats.
- Integrate theoretical knowledge, technical skills, and ethical awareness to propose and implement AI-enabled strategies for defending against cyber threats.

LEARNING OUTCOMES

Upon completion of this course, students will be able to:

1. **Construct AI-Driven Detection Systems:** Develop and optimize functional machine learning models using Python and standard libraries (e.g., Scikit-learn, TensorFlow, PyTorch) to detect specific cybersecurity threats, including phishing attempts, malware signatures, and network anomalies.
2. **Engineer End-to-End ML Pipelines:** Implement complete data pipelines appropriate for security contexts, demonstrating proficiency in data preprocessing, feature engineering, and model training within a practical cybersecurity framework.

3. **Operationalize Defense Models (MLOps):** Design deployment strategies that incorporate MLOps best practices, focusing on model lifecycle management, continuous performance monitoring, and model retraining in response to drifting threat landscapes.
4. **Evaluate Model Robustness and Efficacy:** Critically assess the performance of AI defensive solutions against realistic metrics and adversarial conditions to determine their operational viability and limitations in a live security environment.
5. **Formulate Ethical Governance Strategies:** Analyze the ethical, legal, and societal implications of deploying AI in cybersecurity to create governance frameworks that ensure algorithmic fairness, accountability, and transparency.

LEARNING MATERIALS

- **Mandatory Textbook:** AI-Powered Cybersecurity: Building Intelligent Defense Systems, Techniques and Applications by ElMouatez Karbab (2026) (<https://books.karbab.net/ai-cybersec/>)
- **Optional:** Hands-On Artificial Intelligence for Cybersecurity: Implement smart AI systems for preventing cyber attacks and detecting threats and network anomalies by Alessandro Parisi.
- **Optional:** Hands-On Machine Learning for Cybersecurity: Safeguard your system by making your machines intelligent using the Python ecosystem by Soma Halder and Sinan Ozdemir.
- **Optional:** Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems by Aurélien Géron.

METHODOLOGY

This course includes lectures, discussions, practical applications, group activities, research, and academic reports. Learners contribute to the educational process by being involved by reading and analyzing research related to lecture topics and enriching the discussion through critical evaluation of research and proposed scientific materials. The scientific material of the course, as well as the various references and research, will be provided to the learners on the electronic platform so that they can view it and provide them with the opportunity through weekly lectures to absorb various concepts and discuss readings. The learner is expected to contribute actively to the educational process and will evaluate various activities related to the course such as participation during lectures, critical discussion of research, theoretical and practical assignments.

ACTIVITIES PROCESS

- The need for active participation in the classroom and in the various work teams, and regularity in attending lectures and respecting their schedules starting and ending, as well as not using mobile phones, staying calm and not exchanging side conversations.
- All learners should take great care in completing and submitting requirements on time.
- All learners should treat additional weekly readings with great care to understand, analyze and develop their knowledge by looking for other sources.
- All learners must form a subject file.
- Learners are expected to write down the necessary knowledge during the lecture.

EDUCATIONAL PROCESS

1. **Learner Engagement** Classroom participation and lecture attendance is an active element for every student at the Jawaan Bin Jassim Academy for Defense Studies, and the student is expected to attend all lectures. If the student exceeds the permissible percentage of absence, which is 25%, he will receive a failure grade regardless of his performance. It is the student's responsibility to monitor his attendance. Attendance will be recorded starting from the first day of school, regardless of the period allocated for dropping and adding courses.
2. **Violation of intellectual and moral rights** Violation of intellectual and moral rights is considered academic abuse and may result in the loss of grades or failure. These violations include the following issues and apply to all learners' work:
 - Use the works, ideas, images, or words of any other person without their permission or without reference to the source.
 - Use someone else's name, sentence, paragraph, or article without using quotation marks.
 - Misuse of used sources.
3. **Cases of late delivery or non-delivery of duties**
 - The student who was unable to attend the exam, submit the project or make presentations on time without permission or medical excuse, the evaluation score in that part will be according to the rules of procedure of the Jawaan Bin Jassim Academy for Defense Studies.
 - If the learner is unable to do an assignment due to an acceptable excuse, he will receive an "incomplete" grade in that assessment and will be given another assessment or extension period.

4. **Conduct** The Academy expects learners to adhere to high standards of code of conduct in their interaction with course professors, their colleagues, and the academy community, according to the rules of procedure of the Joaan Bin Jassim Academy for Defense Studies.

ASSESSMENT AND GRADING

A number of different assessment tools will be used to measure the achievement of the aforementioned learning outcomes, including tests, classroom participation and labs.

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

Grading Scale:

Grade	Description	Percentage	Points Earned
A	Excellent	90-100	4.00
B+	Very Good (high)	85 to <90	3.50
B	Very Good	80 to <85	3.00
C+	Good (high)	75 to <80	2.50
C	Good	70 to <75	2.00
F	Fail	Less than 70	0.00
P+	Pass		
P	Pass		
I	Incomplete		
IP	Continuing course		
TC	Transfer Credit		
W	Withdrawal		
WF	Forced Withdrawal		
AU	Audit		

LEARNING AND RESEARCH RESOURCES

All students are required to register with the Qatar National Library (<https://www.qnl.qa/en>), which provides access to most international electronic databases across all scientific disciplines and languages. Relevant databases can be found at <https://qnl.libguides>.

[com/az.php](#), including "Dar Almandumah," "Al Manhal," and databases for theses and dissertations in Arabic. The library also offers access to renowned databases such as Taylor & Francis, ProQuest, Military Database, JSTOR, and Sage Journals.

COURSE SCHEDULE

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
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	

REFERENCES

- [1] Microsoft. (2025). *Microsoft Digital Defense Report 2025* [PDF]. Retrieved from <https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/>

- microsoft/bade/documents/products-and-services/en-us/security/CISO-Executive-Summary-MDDR-2025.pdf
- [2] European Union Agency for Cybersecurity (ENISA). (2025, October). *ENISA Threat Landscape 2025* [PDF]. Retrieved from <https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%202025.pdf>
 - [3] Google Cloud. (2025). *Cybersecurity Forecast 2026* [PDF]. Retrieved from <https://services.google.com/fh/files/misc/cybersecurity-forecast-2026-en.pdf>
 - [4] IBM Security. (2025). *Cost of a Data Breach Report 2025* [PDF]. Retrieved from https://www.bakerdonelson.com/webfiles/Publications/20250822_Cost-of-a-Data-Breach-Report-2025.pdf
 - [5] National Institute of Standards and Technology. (2024, July). *Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile (NIST AI 600-1)* [PDF]. U.S. Department of Commerce. Retrieved from <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf>