JÖNKÖPING UNIVERSITY
School of Engineering

COURSE SYLLABUS

Cybersecurity and AI, 7.5 credits

Cybersäkerhet och AI, 7.5 högskolepoäng

Course Code:	T2COAE	Education Cycle:	Second-cycle level
Confirmed:	Sep 01, 2025	Disciplinary domain:	Technology
Valid From:	Aug 31, 2026	Subject group:	Computer Technology
		Specialised in:	A1F Second cycle, has second-cycle course/s as entry requirements
		Main field of study:	Computer Science

Intended Learning Outcomes (ILO)

On completion of the course the student shall:

Knowledge and understanding

- demonstrate comprehension of fundamental AI concepts relevant to cybersecurity
- display knowledge of how Artificial Intelligence (AI) and Machine Learning (ML) methods can be exploited by adversaries for offensive purposes
- display knowledge of how AI and ML can be employed defensively to detect and mitigate cybersecurity threats

Skills and abilities

- demonstrate skills in identifying and analysing AI/ML-driven cybersecurity threats such as phishing, deepfakes, and automated attacks
- demonstrate the ability to apply AI/ML methods for log analysis, anomaly detection, and intrusion detection

Judgement and approach

- demonstrate the ability to critically assess the ethical implications of using AI in cybersecurity
- demonstrate an understanding of the strengths and limitations of AI/ML methods in cybersecurity contexts

Content

The course provides a comprehensive overview of the intersection of cybersecurity and AI. It introduces core AI and ML concepts and their applications within the cybersecurity domain. It covers how adversaries exploit AI technologies to conduct sophisticated cyber-attacks such as personalised phishing, deepfake generation, and automated hacking techniques. Concurrently, the course explores defensive strategies utilizing AI/ML, including anomaly detection, behavioral analytics, and automated log analysis for threat detection and incident response.

The course includes the following elements:

- Fundamentals of AI and ML
- AI/ML-driven offensive cybersecurity techniques (e.g. personalized phishing and social engineering, deepfakes and misinformation, automated attack strategies,
- AI/ML-driven defensive cybersecurity techniques (e.g. intrusion detection systems, behavioral and anomaly detection, automated analysis and response, and ethical and societal impacts of AI in cybersecurity

Type of instruction

Lectures, seminars, and project work.

Language of instruction is English.

Entry requirements

Passed courses at least 90 credits within the major subject in Computer Science, Informatics, Information Systems, Computer Engineering, or the equivalent, and taken course Cybersecurity Overview, 7,5 credits or the equivalent. Proof of English proficiency is required.

Examination and grades

The course is graded 5, 4, 3 or U.

Registration of examination:

Name of the Test	Value	Grading
Examination [1]	4 credits	5/4/3/U
Project	3.5 credits	G/U

[1] Determines the final grade of the course, which is issued only when all course units have been passed.

Course literature

Please note that changes may be made to the reading list up until eight weeks before the start of the course.