

# WM3F4-15 AI and Cyber Security

**27/28**

**Department**

WMG

**Level**

Undergraduate Level 3

**Module leader**

Christo Panchev

**Credit value**

15

**Module duration**

10 weeks

**Assessment**

100% coursework

**Study location**

University of Warwick main campus, Coventry

---

## Description

### Introductory description

AI-based solutions are having a significant impact in a number of areas, including cyber security. This module will provide students with an in-depth understanding of the main machine learning models, and their practical application in both offensive and defensive cyber operations. This module is designed to develop students not just as a builder of AI-powered defences, but as a critical thinker who understands how these systems can be deceived, subverted, and attacked. We'll explore the dual-use nature of AI, where the same techniques used to detect threats can be repurposed for sophisticated offensive campaigns.

### Module aims

The module aim to develop student's knowledge of the development and application of the most common machine learning models, and in particular a critical understanding of the applicability of each machine learning algorithms in the solution of a particular problem (class of problems). It will cover the best practice and main steps of developing secure AI-based solutions, including data collection/engineering and pre-processing, model design, training and evaluation, and deployment.

### Outline syllabus

This is an indicative module outline only to give an indication of the sort of topics that may be

covered. Actual sessions held may differ.

Some of the main topics covered in the module include:

Methodology of developing an AI-based solution

Exploratory data analysis, feature engineering and pre-processing

Unsupervised learning (clustering) models, such as k-means, nearest neighbour

Supervised learning models, such as linear/logistic regression, decision trees, random forest, SVM

Neural Networks (Deep learning) models, such as MLP, CNN, LSTM

Auto encoders

Generative AI

Security of AI

## Learning outcomes

By the end of the module, students should be able to:

- Critically analyse an application domain and applicability of machine learning models in solving a specific problem. (AHEP4 2.1.1, 2.1.6, 2.1.10, 2.1.13, 2.2.2, 2.3.2, C3, C4, C13)
- Collect, engineer and pre-process real-world data suitable for building machine learning models. (AHEP4 2.1.2, 2.1.7, 2.1.13, 2.2.6, C6, C12)
- Develop, secure and optimise the performance of a machine learning model. (AHEP4 2.1.2, 2.1.7, 2.1.8, 2.1.12, 2.2.1, 2.2.6, C3, C6, C12)
- Evaluate and interpret the results of a machine learning model. (AHEP4 2.1.6, 2.1.7, 2.1.10, 2.1.11, 2.1.13, 2.2.2, 2.3.2, C3, C4)

## Indicative reading list

[Reading lists can be found in Talis](#)

## Subject specific skills

Data analysis

Decision support automation

Application of A.I. if offensive and defensive cyber operations

## Transferable skills

Critical thinking

Analytical thinking

---

## Study

## Study time

| Type                          | Required                    |
|-------------------------------|-----------------------------|
| Lectures                      | 10 sessions of 1 hour (7%)  |
| Supervised practical classes  | 20 sessions of 1 hour (13%) |
| Online learning (independent) | 10 sessions of 1 hour (7%)  |
| Private study                 | 50 hours (33%)              |
| Assessment                    | 60 hours (40%)              |
| Total                         | 150 hours                   |

## Private study description

Additional lab work and research

## Costs

No further costs have been identified for this module.

---

## Assessment

You must pass all assessment components to pass the module.

### Assessment group A

|                                                                                  | Weighting | Study time | Eligible for self-certification |
|----------------------------------------------------------------------------------|-----------|------------|---------------------------------|
| Assessment component                                                             |           |            |                                 |
| Machine Learning Test                                                            | 30%       | 18 hours   | No                              |
| An online test with a combination of multiple choice and short answer questions. |           |            |                                 |

Reassessment component is the same

|                                                                                                                                                                                                                                                                          |     |          |                 |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|----------|-----------------|
| Assessment component                                                                                                                                                                                                                                                     |     |          |                 |
| Machine learning coursework                                                                                                                                                                                                                                              | 70% | 42 hours | Yes (extension) |
| Students will be provided with a data set and tasked with developing a machine learning model solving a particular problem. They will be expected to justify their choice of the specific machine learning model, as well as analyse and evaluate the proposed solution. |     |          |                 |

**Weighting**

**Study time**

**Eligible for self-  
certification**

Reassessment component is the same

## **Feedback on assessment**

Individual marks and cohort feedback for the test, and the standard assessment feedback form for the coursework.

---

## **Availability**

## **Courses**

This module is Core for:

- UWMA-H651 Undergraduate Cyber Security
  - Year 3 of H651 Cyber Security
  - Year 3 of H651 Cyber Security
  - Year 3 of H651 Cyber Security