COURSE DESCRIPTION

Applications of AI to Cyber-threat Management

Academic year 2026-2027

1. Programme-related data

1.1. Higher Education Institution	Babeș-Bolyai University
1.2. Faculty	Faculty of Mathematics and Computer Science
1.3. Department	Department of Computer Science
1.4. Field	Computer Science
1.5. Level of study	Master
1.6. Degree programme / Qualification	Artificial Intelligence for Connected Industries
1.7. Form of education	Full time

2. Course-related data

2.1. Course title	Applications of AI to Cyber-threat Management			Course code	MME8240
2.2. Course coordinator	Lect. dr. Mihoc Tudor Dan				
2.3. Seminar coordinator	Lect. dr. Mihoc Tudor Dan				
2.4. Year of study	2	2.5. Semester	3	2.6. Type of assessment	Colloquium
2.7. Course status	Optional			2.8. Course type	Specialisation subject

3. Total estimated time (hours per semester of teaching activities)

3.1. Number of hours per week	2	of which: 3.2. course	1	3.3. seminar/ laboratory/ project	0/0/1
3.4. Total of hours in the curriculum	28	of which: 3.5. course	14	3.6. seminar/ laboratory/ project	0/0/14

Time allocation for individual study (IS) and self-taught activities (ST)	**hours**
Learning from textbooks, course materials, bibliography, and notes (IS)	12
Additional research in the library, on subject-specific electronic platforms, and on-site	12
Preparing seminars/ laboratories/ projects, assignments, reports, portfolios, and essays	16
Tutoring (professional guidance)	5
Examinations	2
Other activities [i.e.: two-way communication with the course coordinator/tutor]	0
3.7. Total hours of individual study (IS) and self-taught activities (ST)	47
3.8. Total hours per semester	75
3.9. Number of credits	3

4. Prerequisites (where applicable)

4.1. curriculum-related	Master programme AI4CI first semester courses
4.2 skills-related	Data communication, Networking, Basic IT security background.

5. Specific conditions (where applicable)

5.1. course-related	Projector
5.2. seminar/laboratory-related	Computers

6.1. Competencies resulting from the completion of the degree programme *(as referred to in the curriculum)*[1]

Professional competencies	
Competency code	**Competency**
CP7	Develop software
CP33	Innovate in ICT
CP35	Creatively use digital technologies
Transversal competencies	
Competency code	**Competency**
CT1	Think analytically
CT2	Apply knowledge of science, technology and engineering
CT4	Solve problems

6.2. Learning outcomes relevant to the degree programme (as referred to in the curriculum)[2]

Learning outcomes targeted by the subject		
Competency code	**Knowledge and comprehension**	**Specific academic skills**
CP28 CP29 CP30 CP31	The graduate can apply advanced knowledge in artificial intelligence, machine learning, robotics and networks, being able to offer implementation solutions for applications in connected industries.	The graduate has the ability to communicate and develop professional relations and partnerships with industrial partners and with all actors involved in the development process of software and solutions based on artificial intelligence, network architectures and IoT systems .

7. Subject-specific learning outcomes (referred to by each subject coordinator across the range of competencies and learning outcomes at the level of the degree programme)

Knowledge and comprehension
1. Understanding the main concepts of cybersecurity, cybercrime, and cyber-risk management in IT and OT systems.
2. Understanding the operational impact of cybersecurity threats in connected industrial environments.
3. Understanding the role of artificial intelligence and machine learning in cybersecurity, including threat detection, event analysis, and traffic analysis.
4. Understanding current trends, challenges, and opportunities related to AI-based cyber-threat management.
Specific academic skills
1. Analysing cybersecurity scenarios and identifying relevant cyber-risks in IT, OT, and connected industrial contexts.

[1] The professional and/or transversal skills targeted by the subject for which the course description is prepared will be copied from the curriculum of the degree programme. For each competency, the complete entry, including the competency code, will be copied with the exact wording that appears in the curriculum, without any changes. If no competency is copied from either of the two categories, the row corresponding to that category is deleted from the table.

[2] The learning outcomes relevant for the degree programme and targeted by the subject for which the course description is prepared will be listed. The entries, copied without any changes from the Curriculum by subject type (Core Subject/Specialisation Subject/Complementary Subject), are listed under the corresponding competency.

2. Applying AI and machine learning concepts to practical use cases for threat detection and prevention.
3. Document and present case studies, best practices, challenges, and opportunities concerning the use of AI in cybersecurity
4. Preparing reports on laboratory or practical exercises and communicating cybersecurity findings clearly and responsibly.

8. Contents

8.1. Course	**Teaching and learning methods**	**Remarks[3]**
• Understanding security of IT (Informational Technology) and OT (Operational Technology) systems and its impact on industrial operational aspects. • Applications in Connected Industries. • The growing importance of AI and ML in the cybersecurity landscape.	• Interactive exposure • Presentation • Explanation • Practical examples	
Bibliography		
Slides will be distributed.		
8.2. Seminar/ laboratory	Teaching and learning methods	Remarks
• Understanding security of IT (Informational Technology) and OT (Operational Technology) systems and its impact on industrial operational aspects. • Introduction to IT security and OT security. • Cybersecurity and cybercrime: the problems, their evolution, their trends. • The impact of cybercrime. • Applications in Connected Industries. • Industry 4.0 and the digital transformation. • Supply chain attacks. • AI as the core of events and traffic analysis, for threat detection and prevention. • The growing importance of AI and ML in the cybersecurity landscape. • Case Studies and Best Practices. • Challenges and Opportunities.	• Interactive exposure • Explanation • Conversation • Didactical demonstration	
Bibliography		
Slides will be distributed.		

9. Evaluation

[3] For example, organisational aspects, recommendations for students, specific aspects relating to the course/seminar, such as inviting experts in the field, etc.

Type of activity	9.1 Evaluation criteria[4]	9.2 Evaluation methods[5]	9.3 Percentage in the final grade
9.4. Course	Understanding the main elements of Applications of AI to Cyber-threat Management.	Reports on the laboratory/practical exercises	100%
9.5. Seminar/ laboratory	Apply the acquired concepts in practical activities and demonstrate the ability to document and report the obtained results.	Assessment of practical activities and submitted reports.	included
9.6 Minimum standard for passing: Each student should obtain a minimum grade of 5 for the final grade.			

10. SDG labels (Sustainable Development Goals)[6]

	○	Sustainable Development Generic Label						
								
○	○	○	○	○	○	○	○	✔
								No label applies
○	○	○	○	○	○	○	○	○

Date of entry:
20.05.2026

Signature of course coordinator
Lect. dr. Mihoc Tudor Dan

Signature of seminar coordinator
Lect. dr. Mihoc Tudor Dan

Date of approval in the department:
.....

Signature of the head of department
Assoc. Prof. dr. Adrian Sterca

[4] The evaluation criteria must directly reflect the learning outcomes targeted at the level of the degree programme respectively at the level of the subject. More specifically, the learning outcomes set out in the expected learning outcomes are assessed.

[5] Both final evaluation methods and ongoing evaluation strategies should be established.

[6] Select a single label which, according to the *Implementation of SDG labels in the academic process*, best matches the subject. If the subject addresses sustainable development in a generic manner (i.e. by presenting/introducing the general framework of sustainable development, etc.), then the Sustainable Development generic label may be applied. If none of the labels describe the subject, select the last option: *"No label applies."*