Laurea / B.A.
in Global Governance

Academic Year 2024-2025

Workshop Syllabus

Artificial Intelligence & Cybersecurity: Economic & Social Impact, Risk Governance

№ OF SESSIONS: 8 for 16 hours Lecturer

Dr Pamela Pace, entrepreneur

Course Description

Artificial Intelligence (AI) and cybersecurity are transforming the global economic and social landscape, reshaping business models, labor market dynamics, and risk governance strategies. This course provides an in-depth analysis of the strategic implications of these emerging technologies, focusing on how organizations can understand their potential to create value, mitigate risks, and comply with regulations.

Through a multidisciplinary approach, the course will explore AI's role in digital transformation, showcasing how process automation, predictive analytics, and data optimization can contribute to sustainable competitive advantages. At the same time, the evolving cyber threats landscape and the importance of robust security strategies to protect corporate data and assets will be analyzed.

A central focus of the course will be the social and economic impact of AI and cybersecurity, including effects on the labor market, privacy concerns, and consumer trust. We will discuss how governments and businesses are tackling the ethical and regulatory challenges related to the responsible use of these technologies, with a focus on key regulations such as the GDPR and the AI Act.

By examining real-world case studies, featuring industry expert testimonials, and adopting a critical approach, students will gain insights into the opportunities and challenges of digitalization. They will develop a critical understanding to assess the implications of new technologies on business models and society.

This course is designed for economics students and related fields who wish to gain a critical and applicable understanding of emerging trends, equipping themselves with the skills needed to understand the future of work and understand digital governance successfully.

Course Objectives

By the end of the course, participants will be able to:

- **Understand the fundamental concepts and evolution of artificial intelligence and cybersecurity**, with a focus on economic and social impacts.
- **Understand how AI and cybersecurity can be integrated into business models** and analyze strategies to address digital challenges.
- **Gain awareness of key tools and metrics used to evaluate the impact and return on investment (ROI)** of AI and cybersecurity solutions.
- **Reflect on the ethical and sustainable aspects of AI**, understanding the regulatory and social implications related to the responsible adoption of these technologies.

- **Analyze concrete case studies**, evaluating successes and failures in AI and cybersecurity adoption to draw practical lessons.
- **Assess the impact of AI on privacy and security**, identifying major digital threats and effective mitigation strategies.
- **Explore the existing regulatory framework (GDPR, AI Act, etc.)**, and understand how regulations influence business processes and decision-making.
- **Analyze emerging trends in AI and cybersecurity and their potential impact** on businesses and society.
- **Promote a culture of cybersecurity**, raising awareness on the importance of data protection and digital resilience.
- **Link AI and cybersecurity to the job market**, analyzing opportunities and challenges related to digital transformation.

Course Format
The course will follow an interactive format, alternating between:

- **Interactive lectures** to introduce and contextualize key concepts.
- **Case study discussions** to explore real-world applications and challenges.
- **Group exercises** to analyze and mitigate AI and cybersecurity risks.
- **Guest speaker sessions** featuring industry leaders sharing their insights and experiences.
- **Quizzes and assessments** to consolidate learning.

The course consists of 16 total hours, spread across four consecutive days, with two sessions per day lasting two hours each.

Syllabus Breakdown
Day 1: Foundations of AI and Cybersecurity

Morning (11:00 - 13:00): Introduction to AI

- Historical evolution and future trends.
- Key applications in business and economics.
- Societal opportunities and risks.

Afternoon (14:00 - 16:00): Foundations of Cybersecurity

- Overview of digital threats (data breaches, ransomware, phishing).
- The role of cybersecurity in fostering digital trust.
- Case studies: Successful and failed approaches in managing AI and cybersecurity.

Day 2: Governance and Regulation

Morning (11:00 - 13:00): Governance Frameworks

- AI governance principles: Transparency, accountability, and fairness.
- Cybersecurity frameworks: ISO 27001, NIST.
- Challenges in implementing governance models.

Afternoon (14:00 - 16:00): Global Regulations

- GDPR and AI Act: Key takeaways and implications for businesses.
- Comparative analysis of global AI regulations.
- Case study: Regulatory responses to AI-related incidents.

Day 3: Social and Economic Impacts

Morning (11:00 - 13:00): AI and the Labor Market

- Automation vs. job creation: Navigating transitions.
- Strategies for upskilling and reskilling.
- Case study: How industries adapt to AI-driven change.

Afternoon (14:00 - 16:00): Cybersecurity and Social Trust

- Costs and consequences of cyberattacks.
- Ethical considerations in cybersecurity.
- Discussion: Future challenges in a hyper-connected world.

Day 4: Strategic Integration and Emerging Trends

Morning (11:00 - 13:00): Leveraging AI in Business

- Integrating AI into business strategies.
- Measuring ROI: Key performance indicators (KPIs) for AI adoption.
- Case study: Successful AI implementation stories.

Afternoon (14:00 - 16:00): Emerging Trends and Innovations

- Generative AI: Opportunities and risks (e.g., ChatGPT, deepfakes).
- Future trends in AI and cybersecurity.
- Workshop: Group discussions on strategic recommendations for businesses.

Assessment Methods
Participants will be assessed through:

- **Daily quizzes**, short interactive tests to consolidate knowledge.
- **Practical exercises**, simulations of risk analysis and real-world case studies.
- **Active participation**, engagement in discussions and workshops.

Schedule Overview – Daily Breakdown

Day	Time	Main topics
Monday	11:00 - 13:00	Introduction to AI and cybersecurity: Key concepts and business applications.
	14:00 - 16:00	Economic and social impacts of AI: Opportunities and challenges for businesses and society.
Tuesday	11:00 - 13:00	Cybersecurity threats: Ransomware, data breaches, and digital fraud.
	14:00 - 16:00	Compliance and regulations: GDPR, AI Act, and other regulatory frameworks.
Wednesday	11:00 - 13:00	AI and employment: Automation, new skills, and workforce impacts.
	14:00 - 16:00	AI ethics and biases: Impacts on business decisions and society.
Thursday	11:00 - 13:00	Integrating AI and cybersecurity in business strategies: Practical approaches and success metrics.
	14:00 - 16:00	Case study analysis and final discussion: Lessons learned and future challenges.

Expected Outcomes

At the end of the course, students will be able to:

- Understand the importance of AI and cybersecurity in business and economic contexts.
- Critically analyze the risks and opportunities associated with these technologies.
- Understand key regulatory frameworks and governance models for mitigating technological risks.
- Understand the role of AI and cybersecurity in business models and assess their potential applications.
- Measure the value of technologies through appropriate tools and metrics.
- Recognize and address the ethical and social implications of AI.
- Recognize key factors influencing the return on investment (ROI) of digital technologies.
- Collaborate in multidisciplinary teams to address digital challenges.

E-mail

pacepamsam@gmail.com