Cybersecurity Strategies in the Era of Artificial Intelligence

Blended Intensive Program

The Program discusses the most important aspects relating to cybercrime and cybersecurity from an interdisciplinary perspective. This Program uses lectures, utilizes legal and business cases, academic studies, and international organizations reports, and employs participatory learning. The Program will consist of five modules, as follows.

Module 1 covers essential concepts regarding cyberspace, technologies, and cybercrime trends; types of cybercrime; cybercrime personal, economy, and national security impacts; the General Data Protection Regulation; the Cybercrime Convention; the Electronic Commerce Directive; Directive (EU) 2019/790; the Directive (EU) 2019/770; Directive (EU) 2016/1148; the United Nations Convention against Transnational Organized Crime; risk-related concepts; foundations of information security; general aspects concerning cybersecurity.

Module 2 covers typologies of cybercrime, with in-depth analysis of offences against the confidentiality, integrity, and availability of computer data and systems computer-related offences, and content-related offences.

- Illegal access
- Illegal interception
- Forms of computer damage
- Types of computer frauds
- Computer-related identity offences
- Offences related to infringements of copyright and related rights
- Several real cases are discussed within this Module on computer damage, computer fraud, computer espionage, and trafficking in passwords

Module 3 analyzes interpersonal crime: cyberstalking, cyberharassment, and cyberbullying.

- Define interpersonal cybercrime
- Types of interpersonal cybercrime
- Perpetration of interpersonal cybercrime
- Laws targeting interpersonal crime
- Discussion of several real cases and Metaverse aspects

Module 4 discusses aspects, perspectives, and responses pertaining to hacktivism and disinformation campaigns.

- Hacktivism motivation, methods, and examples
- Disinformation definitions, actual or potential consequences, and laws
- Disinformation formats, methods, and tactics
- Instances of alleged disinformation
- Successful disinformation campaigns

Module 5 explores cybersecurity strategies and the use of AI to prevent and detect cybercrime.

- Legal framework
- Threats, vulnerabilities, and risk assessment
- International cybersecurity cooperation
- AI and innovative models to prevent cyber threats
- Use of AI to address incident response, threat hunting, and data analysis
- Case studies regarding anomaly and intrusion detection machine learning