

Cybersecurity Strategies in the Era of Artificial Intelligence

Description of the virtual component

Prof. Dr. Ioana VasIU

The virtual component comprises an introduction, which reviews key concepts, definitions of terms, and cybersecurity risks and threats. Several real cases are presented and the consequences of these incidents are highlighted. A part of this component is dedicated to the examination of the foremost adversarial goals, vulnerabilities, types of cybercrimes, cybersecurity risk-management measures, and the AI methods employed in the cybersecurity functions. Another part of this component surveys the EU legal framework, followed by the in-depth analysis of the main components, including the Directive (EU) 2022/2555, the Directive (EU) 2022/2557, the Regulation (EU) 2022/2554, the AI Act, and the proposed Regulation on horizontal cybersecurity requirements for products with digital elements. Finally, the module outlines the related international standards and important research papers.