Cybersecurity (MS) with an Emphasis in Artificial Intelligence

This program is offered by the George Herbert Walker School of Business and Technology and is available online via asynchronous modality, at the St. Louis main campus and San Antonio.

Program Description

Education at the graduate level is an expansion of the knowledge attained from undergraduate studies. Graduate education encourages the development of advanced skills, theoretical knowledge and critical thinking skills to practice the art and science of cybersecurity techniques to defend networks and systems, analyze attacks, and conduct forensic evaluations.

Students entering this degree must have an undergraduate degree in Computer Science, Management Information Systems, Information Technology, or a related degree with an understanding of basic software programming, network management, and systems/development operations. Professional experience may be accepted upon evaluation. Additionally, it is important for the student to be proficient in written and oral communication skills.

The master of science (MS) in cybersecurity with emphasis in artificial intelligence prepares individuals for demanding positions in public and private sectors analyzing, managing, operating, or protecting critical computer systems, information, networks, infrastructures and communications networks.

Students will be well-versed to apply their knowledge and critical thinking related to social engineering techniques, network defenses, online malware methods, critical infrastructure protection, fraud, theft, digital forensics, and threat detection.

A background on Artificial Intelligence and Machine Learning will be provided and the potential benefits of the technology in multiple areas will be described. Python will be introduced and used to resolve AI-related questions. The program will introduce Deep Learning and provide an understanding of many ways in which AI can provide support to multiple disciplines.

Students may not apply for dual majors because of the technical nature of this MS degree program. Students may apply for sequential degrees as long as they do not duplicate core courses.

Learning Outcomes

Core Cybersecurity curriculum:

- Capable of explaining important technical methods and theories used throughout the discipline of cybersecurity.
- Capable of applying knowledge in the field of cybersecurity to analyze software and online issues.
- Capable of effectively integrating knowledge in the field of cybersecurity to propose solutions to real-world problems.
- Apply cybersecurity social engineering techniques, as well as deterrence and forensice analysis, to information systems, applications and operation situations.

Artificial Intelligence emphasis:

- Explain the role of data analytics in organizational decision making.
- Utilize current analytical languages to manage key artificial intelligence requirements.
- Explain the fundamental aspects of artificial intelligence and the potential benefits to companies and organizations.
- Develop machine learning techniques and algorithms to resolve key artificial intelligence problems.
- Implement major algorithms and statistical models related to Machine Learning to solve problems in different areas of industry.
- Utilize Deep Learning methods to address topics in multiple disciplines.

Program Curriculum

The 39 credit hours required for the MS in cybersecurity must include the 21 required core courses and the 18 required emphasis courses.

Core Courses (21 hours)

- CSSS 5100 Secure Software Design and Threat Analysis (3 hours)
- CSSS 5120 Cybersecurity Infrastructures (3 hours)
- CSSS 5160 Encryption Methods and Techniques (3 hours)
- CSSS 5180 Social Engineering (3 hours)
- CSSS 5220 Cybersecurity Threat Detection (3 hours)
- CSSS 5230 Cybersecurity Forensics (3 hours)
- CSSS 6000 Practical Research in Cybersecurity (3 hours)