Artificial Intelligence and Cybersecurity

Session 1: 6/10 – 7/8 Asynchronous and 6/16 – 6/17 Synchronous

Session 2: 7/10—8/8 Asynchronous and 7/28 - 7/29 Synchronous

From reengineering manufacturing to self-driving cars, to digital humans *Artificial* Intelligence and Machine Learning have created a new frontier of science and business. There are numerous technologies that fall under the general rubric of AI/ML that we cover in this class. The myriad technological advances based on AI/ML that have resulted in advances to society there are also potential societal dangers that need to be understood and mitigated as the societal footprint of AI grows. The AI-based chatbots are generating credible content that matches up with human writing – with a potential for plagiarism. Generative Adversarial Networks have helped create indistinguishable deep fakes that can help in the manipulation of public opinion. Societal biases from the past have the potential for future discrimination through the codification of historic data in AI systems. The AI systems themselves are subject to cyberattacks – data poisoning, contrived data injection, etc.

SCAN ME

Scan the QR code or follow this link to the registration page.

For more information regarding this class, contact:

Sanjay Goel

* This workshop is limited to faculty and graduate students pursuing a career in teaching cybersecurity.

At the time of registration, all participants must be affiliated with a CAE school and a US citizen or US permanent resident