ICMAT
INSTITUTO DE CIENCIAS MATEMÁTICAS

DataLab

seminar

SECURITY ASPECTS OF MACHINE LEARNING

SPEAKER: Roi Naveiro Flores (ICMAT)

DATE: Thursday, 29 October 2020 - 10:30

PLACE: Aula Azul (ICMAT) and online: https://conecta.csic.es/b/roi-4yv-7z9

ABSTRACT: Recent contributions to the security of Machine Learning will be covered. In particular, a novel proactive defense in Adversarial Supervised Learning problems will be presented. This approach mitigates the effects of the unrealistic common knowledge assumptions, prevalent in standard game theoretic approaches. Algorithmic aspects will be considered as well.

MINISTERIO DE CIENCIA E INNOVACIÓN
CSIC Consejo Superior de Investigaciones Científicas
UAM Universidad Autónoma de Madrid
Universidad Complutense Madrid
uc3m Universidad Carlos III de Madrid
EXCELENCIA SEVERO OCHOA