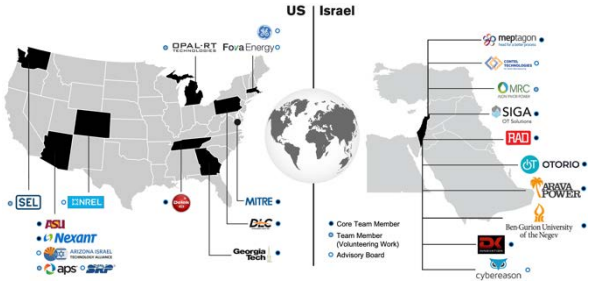
BIRD Israel-U.S. Binational Industrial Research and Development Foundation



U.S.-Israel Energy Center

Converging Cybersecurity Solutions for Energy Systems to Practice

Adversarial AI: A Cyber Security Perspective

Yuval Elovici

Ben-Gurion University

September 6, 2022, 7:00 - 8:00 pm, Israeli time

(12:00-1:00 pm EST, 9:00 am-10:00 am AZ/PST Time)

Link: https://asu.zoom.us/j/6712258140

Abstract: In recent years, machine learning algorithms and, more specifically, deep learning algorithms have been widely used in many fields, including cyber security. However, machine learning systems are vulnerable to adversarial attacks, and this limits the application of machine learning, particularly in dynamic, adversarial environments, such as the cyber security domain where actual adversaries exist. This talk will shed light on the latest research on adversarial attacks against security solutions based on machine learning techniques. It will illuminate the risks they pose while illustrating the feasibility of launching adversarial attacks on security systems in general and cyber security systems. The talk will also provide an overview of attacks on advanced driver assistance systems (ADASs), which are widely used by EVs like Tesla; surveillance systems, which are widely used at airports to detect suspects that appear on a blacklist; and malware classifiers, which are embedded in endpoint EDR and intrusion detection systems widely deployed at large organizations.

Bio:

Yuval Elovici is the director of the Telekom Innovation Laboratories at Ben-Gurion University of the Negev (BGU), head of BGU's Cyber Security Research Center, and a professor in the Department of Software and Information Systems Engineering at BGU. He holds B.Sc. and M.Sc. degrees in computer and electrical engineering from BGU and a Ph.D. in information systems from Tel Aviv University. His primary research interests are computer and network security, cyber security, web intelligence, information warfare, side-channel attacks, AI security, and machine learning. Prof. Elovici also consults professionally in the area of cyber security, sharing his expertise with both startups and large international companies, and is the co-founder of Morphisec, a startup that develops innovative cyber security mechanisms related to moving target defense, and CyberMed which focuses on securing medical imaging devices.