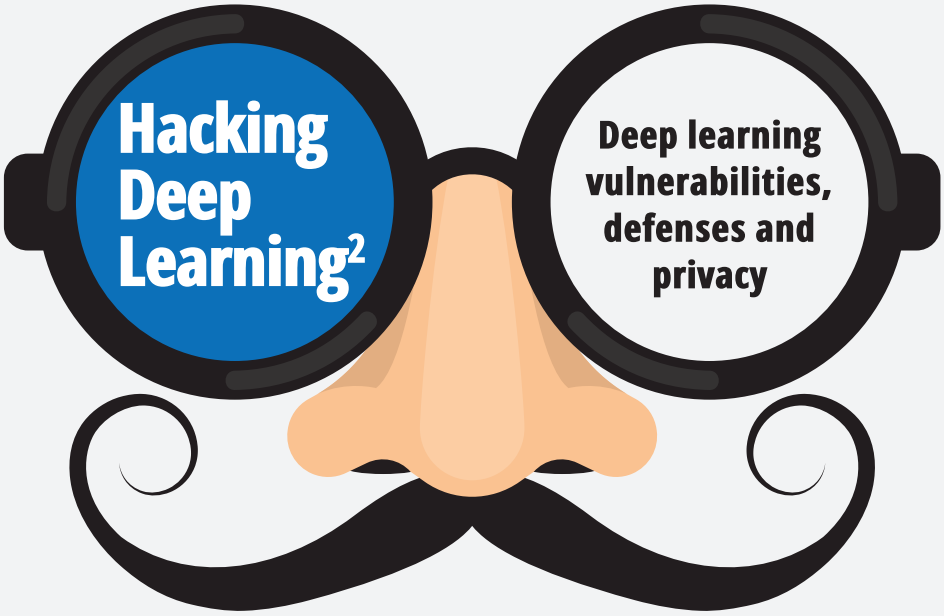
Prime Minister's Office
National Cyber Directorate
National Cyber Bureau

BIU Center for Research in Applied Cryptography and Cyber Security

אוניברסיטת בר-אילן
Bar-Ilan University



January 22, 2019 | 08:30-16:30

Auditorium C50, Nanotechnology Building (bldg. 206), Bar-Ilan University

Organizers: **Benny Pinkas** and **Joseph Keshet**
Department of Computer Science

08:30 – 09:20	Gathering
09:20 – 09:30	Opening remarks
09:30 – 11:00	**Tutorial on Adversarial Machine Learning** Battista Biggio, *University of Cagliari*
11:00 – 11:30	Coffee break
11:30 – 12:15	**Learning with Perturbations** Tamir Hazan, *Technion*
12:15 – 13:45	Lunch
13:45 – 14:30	**A Simple Explanation for the Mysterious Existence of Adversarial Examples with Small Hamming Distance** Adi Shamir, *Weizmann Institute of Science*
14:30 – 15:15	**Cryptography for Privacy-Preserving Machine Learning** Morten Dahl, *tf-encrypted project, Dropout Labs*
15:15 – 15:45	Coffee break
15:45 – 16:30	**Privacy-Preserving Data Analysis: Proofs, Algorithms, and Systems** Adria Gascon, *Alan Turing Institute and University of Warwick*

Registration

Registration fee is 150 ILS for the entire day and includes lunch and refreshments.
For any question/request regarding registration, please contact us at: **cyber.center@biu.ac.il**
Please register by January 10, 2019 at: https://deep-learning.forms-wizard.co.il/users/new

The workshop is organized in collaboration with the Department of Computer Science and is graciously sponsored by the BIU Center for Research in Applied Cryptography and Cyber Security in conjunction with the Israel National Cyber Directorate in the Prime Minster's Office and the Alter family.

CS@BIU DEPARTMENT OF COMPUTER SCIENCE BAR-ILAN UNIVERSITY