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

HACKING DEEP LEARNING

Attacking deep networks by adversarial examples
Differential privacy in machine learning
Forensics

Auditorium C50, Nanotechnology Building (bldg. 206),
Bar-Ilan University
January 29, 2018 | 09:00-18:00

SAVE THE DATE
29/01/18

ORGANIZERS

Joseph Keshet and Benny Pinkas
Department of Computer Science, Bar-Ilan University

SPEAKERS

Moustapha Cisse
Facebook

Nicolas Papernot
Penn State University

Anand Sarwate
Rutgers University

Rita Singh
Carnegie Mellon University

Rita Osadchy
University of Haifa

Bhiksha Raj
Carnegie Mellon University

Vitaly Shmatikov
Cornell Tech

REGISTRATION

Participants from academia, industry, and anyone interested in the security of deep learning are welcome.

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 14, 2018 at: https://deep-learning.form-wizard.biz

This conference is organized in collaboration with the Department of Computer Science and the Data Science Institute at Bar-Ilan University.

CS@BIU DEPARTMENT OF COMPUTER SCIENCE BAR-ILAN UNIVERSITY

DSI Understanding the world through Data Bar-Ilan University