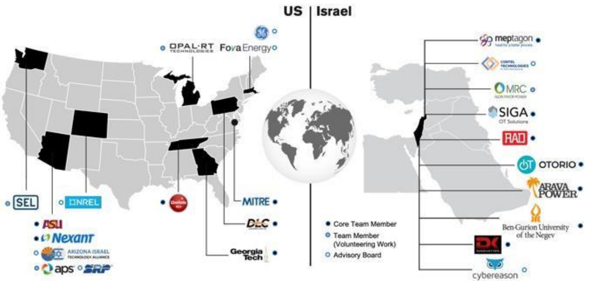
BIRD
Israel-U.S.
Binational Industrial Research
and Development Foundation



U.S.-Israel Energy Center

Converging Cybersecurity Solutions for Energy Systems to Practice

The Threat Horizon of Deepfakes and Their Impact on Organizations

Yisroel Mirsky

Ben-Gurion University (BGU)

March 29, 2023, 7:00 - 8:00 pm, Israeli time

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

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

Abstract: Deep learning has provided us with the ability to automate tasks, extract information from vast amounts of data, and synthesize media that is nearly indistinguishable from the real thing. However, positive tools can also be used for negative purposes. Since 2018, deep learning has been used to re-enact people in `deepfakes' not only for entertainment but for revenge, fraud, and espionage as well. Many companies are concerned about how this impacts their security. With rapid advances in generative AI and the ease of access to the technology, we wonder what is on the horizon regarding malicious deepfakes: what will attacks look like in the near future and how will we prevent them? In this talk, we will talk about different types of deepfakes (e.g., human face/voice, medical records, etc.), how they are made, detected, and their caveats. We will also look into an imminent threat which has recently emerged and give insight into the matter.

Bio:

Yisroel Mirsky is a tenure-track lecturer and Zuckerman Faculty Scholar in the Department of Software and Information Systems Engineering at Ben-Gurion University. He received his Ph.D. from BGU in 2018 and was a postdoctoral fellow for two years in the Georgia Institute of Technology. He currently heads the Offensive AI research lab in BGU https://ymirsky.github.io/Offensive.AI.Lab/
His main research interests include deepfakes, adversarial machine learning, anomaly detection, and intrusion detection. Dr. Mirsky has published his work in some of the best security venues: USENIX, CCS, NDSS, Euro S&P, Black Hat, DEF CON, RSA, CSF, AISec, etc. His research has also been featured in many well-known media outlets: Popular Science, Scientific

American, Wired, The Wall Street Journal, Forbes, and BBC. Some of his works, include the exposure of vulnerabilities in the US 911 emergency services and research into the threat of deepfakes in medical scans, both featured in The Washington Post.