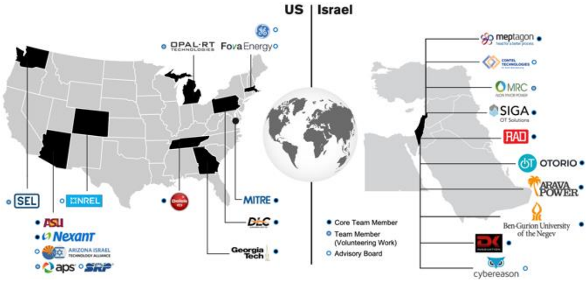
BIRD
Israel-U.S.
Binational Industrial Research
and Development Foundation



U.S.-Israel
Energy Center

Cybersecurity Technology for Critical Power Infrastructure AI-Based Centralized Defense and Edge Resilience

Quarterly Review Workshop II Agenda

May 9, 2022

Israeli Time: 7-10 pm

US Time: 12 - 3 pm (EST), 9 am - 12 pm (Pacific / AZ)

Purpose of Quarterly Review Workshop

Welcome to the BIRD-ICRDE cybersecurity project workshop II. We are delighted to have this opportunity to share with the consortium members some progress updates of this Israel-US binational joint project. This review workshop is a go/no-go meeting in which the progress of each project task will be evaluated. The Principal Investigator(s) of each task will present the research results and discuss their plan for future quarters. The focus of the presentations will be on *tool development*, demonstration of the *practical values and potential impact* of the research, and *commercialization* in collaboration with industry partners. The workshop will be conducted via zoom video conferencing and recorded for future reference. Please use the link below to join.

https://asu.zoom.us/j/9723906777

Agenda (Moderator: Yang Weng) (all times are in Israeli evening time):

7:00-7:05 Project Overview

Data for System Modelling, and State Monitoring and Estimation:

7:05-7:15 Task 1: Realization of advanced energy management applications
John Dirkman (Nexant), Yang Weng (ASU)

7:15-7:25 Task 2: Digital rep. of physical processes & operational process modelling
Asaf Shabtai, Rami Puzis (BGU), Matan Dobrushin (OTORIO)

7:25-7:35 Task 3: Data collection and aggregation
Matan Dobrushin (OTORIO), Rami Puzis (BGU), Yang Weng (ASU)

Knowledge Base and Learning of Cyber Threats:

7:35-7:45 Task 4: Multi-level threat intelligence knowledge base

Adam Hahn, Marie Collins (MITRE), Bracha Shapira, Rami Puzis (BGU)

7:45-7:55 Task 5: GANs for generating adversarial attacks
Lalitha Sankar, Rajasekhar Anguluri (ASU), John Dirkman (Nexant)
7:55-8:05 Task 6: Threat hunting, Rami Puzis (BGU)

Prediction and Detection of Cyber-attacks of IT/OT Systems

8:05-8:15 Task 7: Malware threats mitigation
Wenke Lee, Moses Ike (GIT), Ron Insler, Yuri Gofman (RAD)
8:15-8:25 Task 8: Detect event mimicking attacks
Lalitha Sankar, Rajasekhar Anguluri (ASU), John Dirkman (Nexant)
8:25-8:35 Task 9: False data injection
Hagai Galili, Ilan Gendelman, Adi Bartov (SIGA)
8:35-8:45 Task 10: Multi-layer anomaly detection framework
Nir Nissim, Robert Moskovitch (BGU), Ron Insler (RAD)
8:45-8:55 Task 11: AI based intrusion detection
Yisroel Mirsky (BGU) [5 min], Ying-Cheng Lai (ASU) [5 min]
8:55-9:05 Task 12: Explainable cyber A.I. analytics (10 min.)
Bracha Shapira, Antwarg Liat, Nir Nissim (BGU)

Threat Mitigation and Cyber Resilience

9:05-9:10 Task 13: Firmware verification, Yossi Oren, Michael Amar (BGU)
9:10-9:20 Task 14: Cyberattack tolerance
Sukarno Mertoguno (GIT), Ali Kazemi (Schweitzer Engineering Lab)
9:20-9:30 Task 15: Self-healing and auto-remediation, Asaf Shabtai (BGU)
9:30-9:40 Task 16: Reinforcement learning control for cyber physical systems
Ying-Cheng Lai (ASU)

Future-proof Architectures and Consortium Programs

9:40-9:50 Task 17: ICS security by design, Yuval Elovici (BGU)
9:50-10:00 Task 18: Task 18: Hardware-in-the-loop validation
Yang Weng (ASU), Philippe Bisson (Opal-RT)
10:00-10:05 Task 19: Innovation, education, coordination, and marketing programs
Dan Blumberg, Asaf Shabtai (BGU)
10:05-10:10 Closing Remarks

ICRDE Management Team (Yang Weng, Rami Puzis, Aviad Elyashar, Chin-Woo Tan, Shuman Luo)