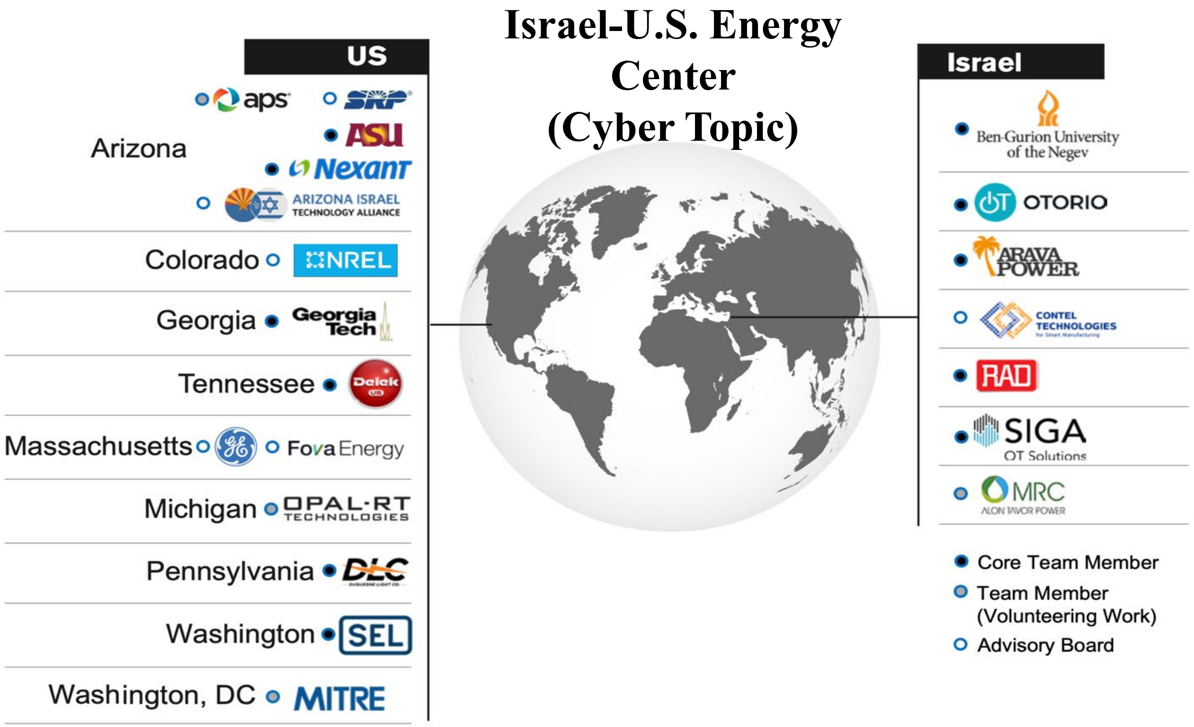
Comprehensive Cybersecurity Technology for Critical Power Infrastructure AI-Based Centralized Defense and Edge Resilience



Prepared for

Itai Ganzer and **Ofer Goldhirsh**

Israel Innovation Authority

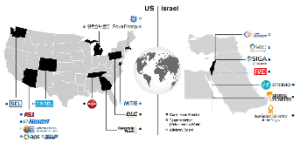
Avi Shavit and **Eynan Lichterman**

Israel Ministry of Energy

Task 11: AI Based Intrusion Detection

Ying-Cheng Lai
Arizona State University
5/9/2022

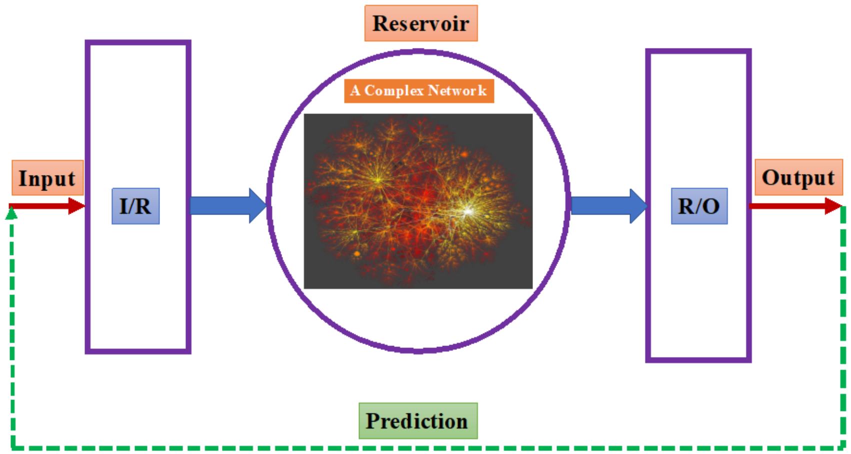
Overview of Task Progress To date



Task 11: AI Based Intrusion Detection					
Pis: Ying-Cheng Lai (ASU), Yisroel Mirsky (BGU)					
Task Milestones	Start Date	End Date	Today	Total Duration in Days	Progress
M11.1 Analysis of enterprise and ICS NIDS software architectures	11/1/2021	10/31/2022	5/9/2022	364	
M11.1 Actual Progress	1/5/2022	10/31/2022	5/9/2022	299	30%
M11.2 Develop digital twin to generate labeled data	11/1/2021	4/30/2023	5/9/2022	545	
M11.2 Actual Progress	1/5/2022	4/30/2023	5/9/2022	480	20%
M11.3 Design attack scenarios for the generation of labeled data	11/1/2021	10/31/2023	5/9/2022	729	
M11.3 Actual Progress	1/5/2022	10/31/2023	5/9/2022	664	15%
M11.4 Design Deep Learning architecture for attack detection	1/5/2023	10/31/2023	5/9/2022	299	
M11.4 Actual Progress	1/5/2022	10/31/2023	5/9/2022	664	10%
M11.5 Design Deep Reinforcement Learning architecture	1/5/2023	10/31/2023	5/9/2022	299	
M11.5 Actual Progress	1/5/2022	10/31/2023	5/9/2022	664	15%
M11.6 Design of a real-time Deepfake Detection Tool	5/1/2022	4/30/2023	5/9/2022	364	
M11.6 Actual Progress	5/1/2022	4/30/2023	5/9/2022	364	
M11.7 Develop prototype for identifying Real-time Deepfakes	4/1/2023	4/30/2024	5/9/2022	395	
M11.7 Actual Progress	4/1/2023	4/30/2024	5/9/2022	395	
Note: Prof. Lai's milestones: M11.1-M11.5; Prof. Mirsky's milestones: M11.6-M11.7					

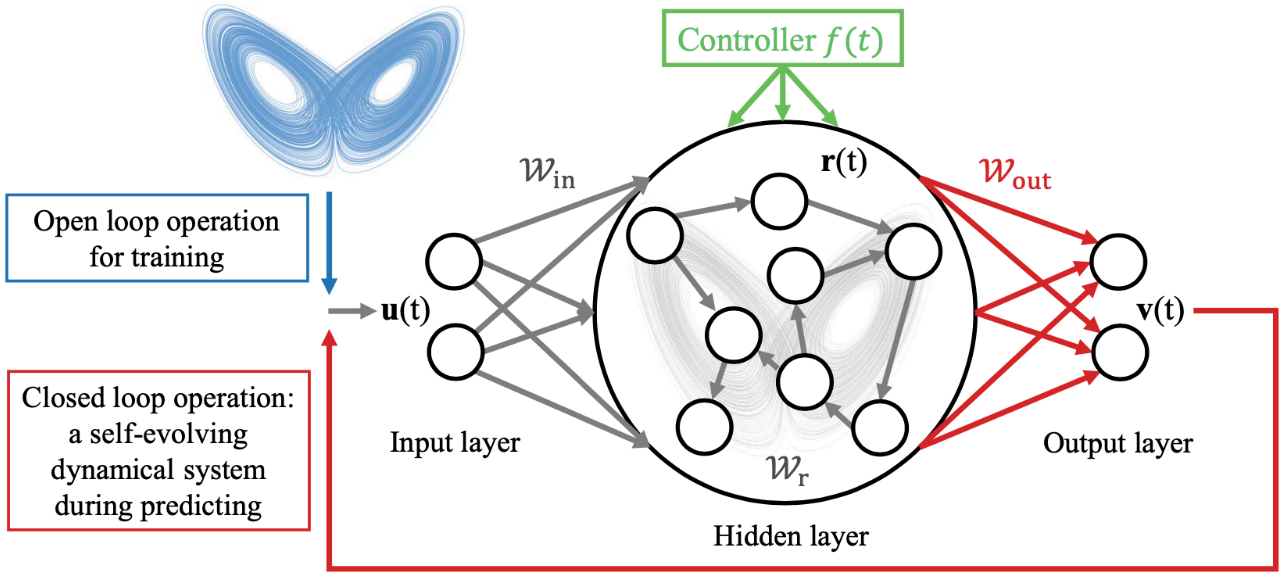
Technical Content: Design Imperatives of Digital Twins

Reservoir computing: general architecture



- H. Jaeger and H. Haas, Harnessing nonlinearity: Predicting chaotic systems and saving energy in wireless communication, *Science* **304**, 78 (2004);
- J. Pathak, B. Hunt, M. Girvan, Z. Lu, and E. Ott, Model-Free Prediction of Large Spatiotemporally Chaotic Systems from Data: A Reservoir Computing Approach, *Phys. Rev. Lett.* **120**, 024102 (2018);
- J. Jiang and Y.-C. Lai, Model-free prediction of spatiotemporal dynamical systems with recurrent neural networks: Role of network spectral radius, *Phys. Rev. Research* **1**, 033056 (2019).

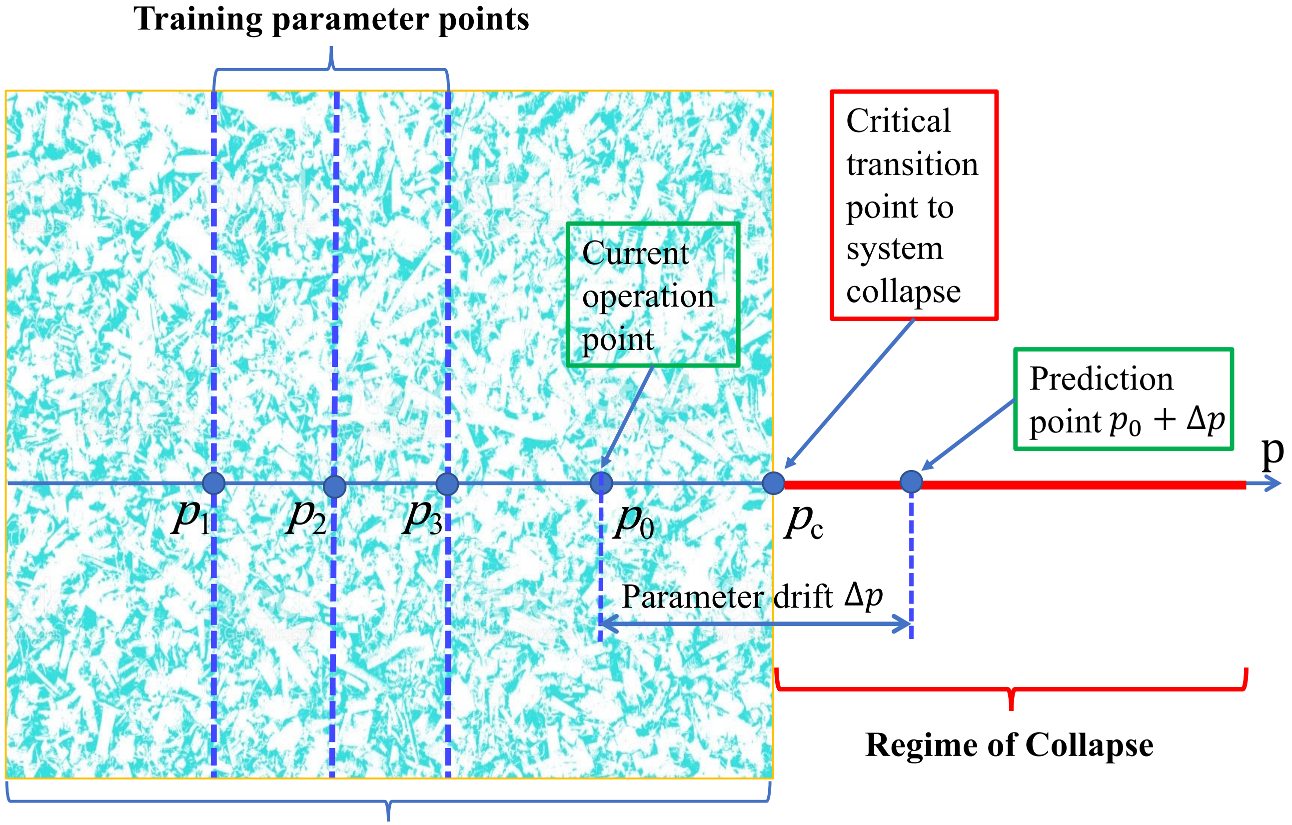
ASU Design: Creation of recurrent neural-network based digital twin



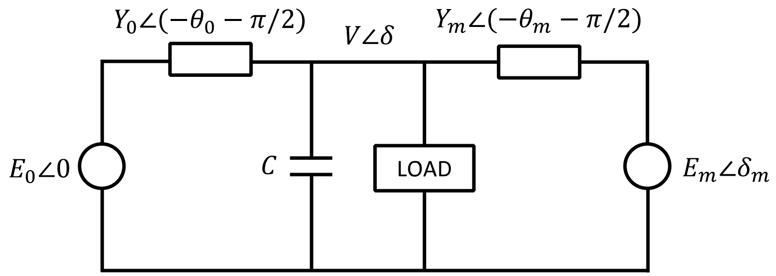
- L.-W. Kong, H.-W. Fan, C. Grebogi, and Y.-C. Lai*, "Machine learning prediction of critical transition and system collapse," *Physical Review Research* **3**, 013090, 1-14 (2021)
- L.-W. Kong, Y. Weng, B. Glaz, M. Haile, and Y.-C. Lai*, "Digital twins of nonlinear dynamical systems," working paper (2022).

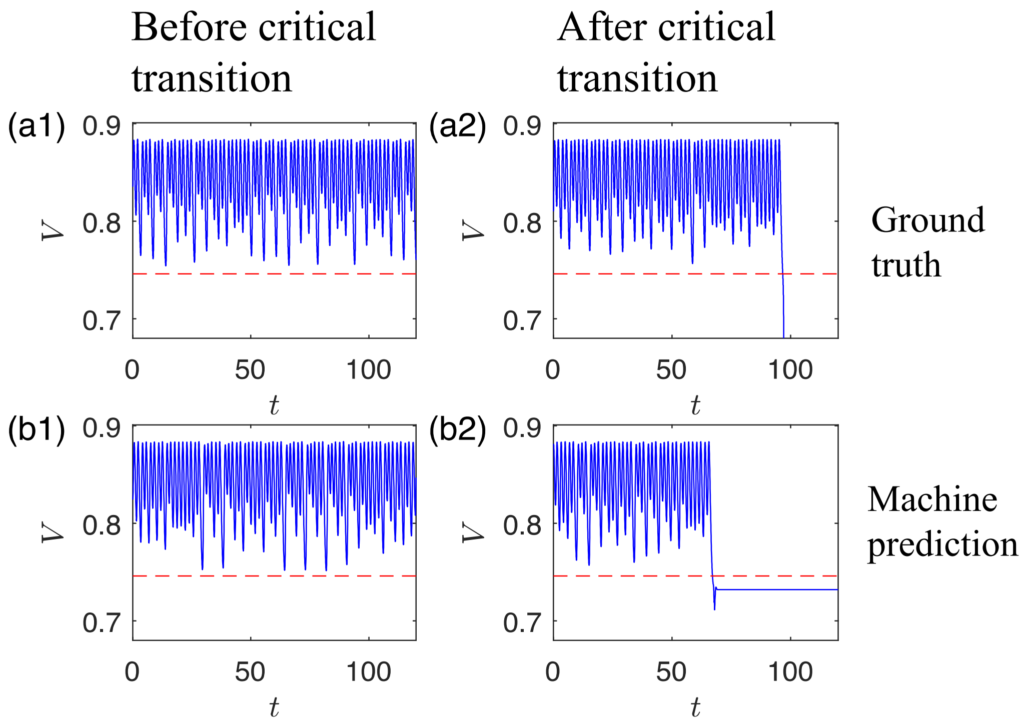
Technical Content: Parameter Adaptable Training of Digital Twins

Parameter-dependent training of digital twin



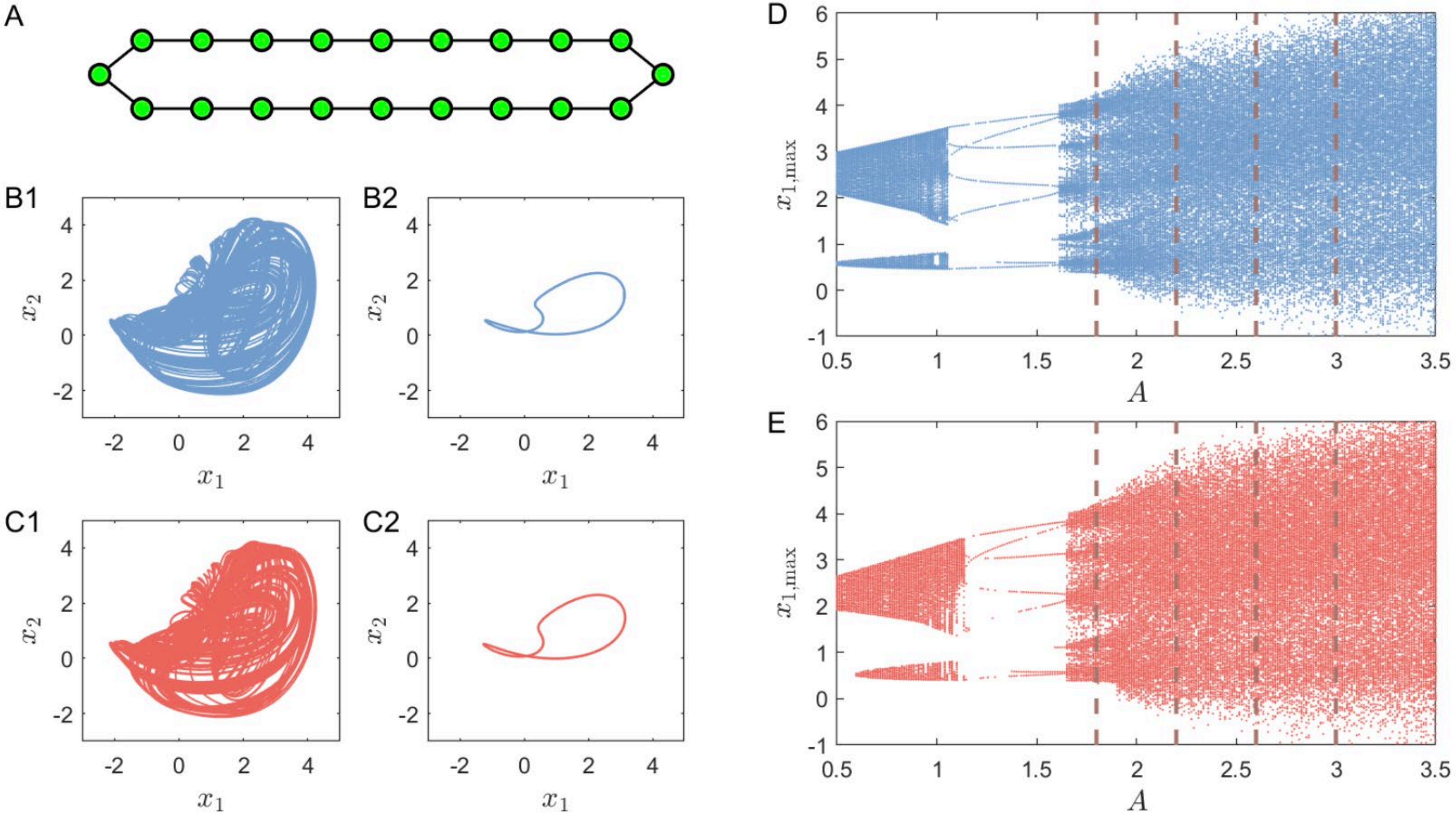
An example





Technical Content: Forecasting Global Dynamics

Lorenz-96 climate network



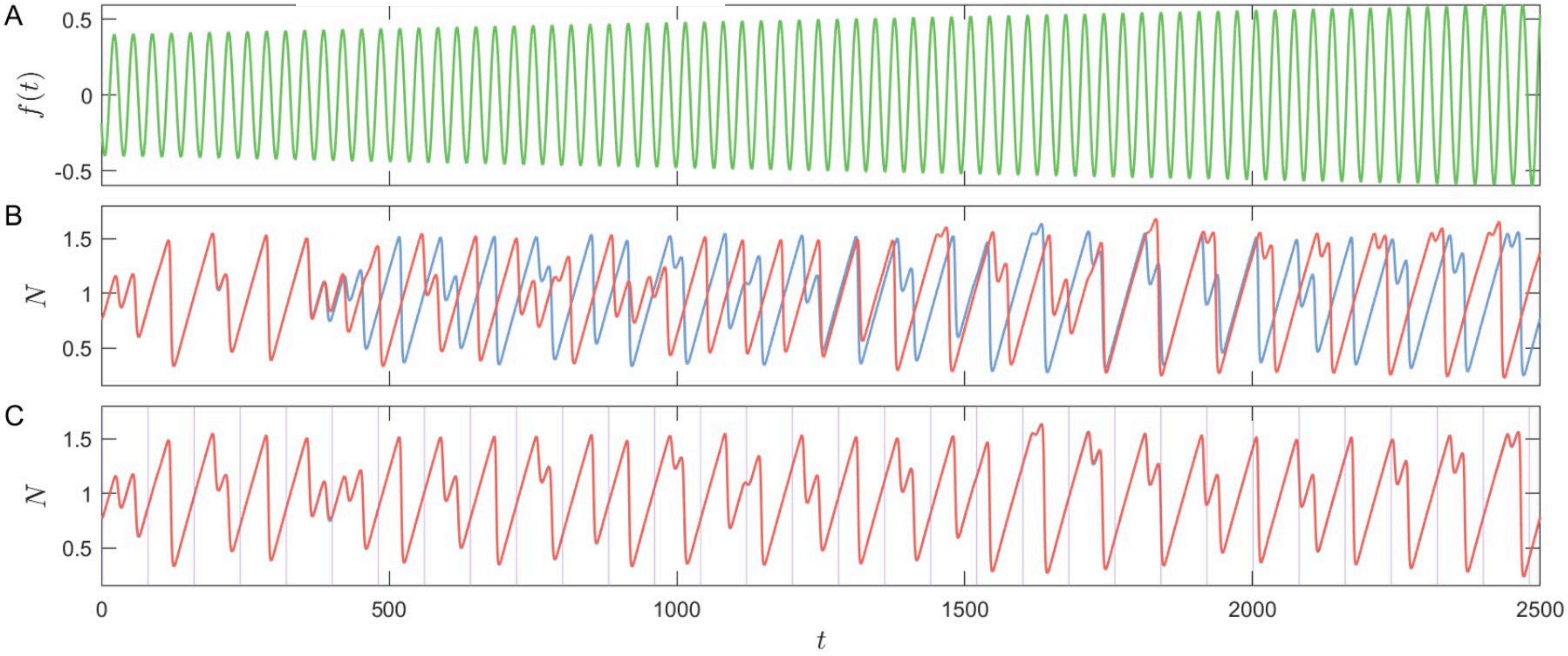
Ground truth

Digital twin prediction

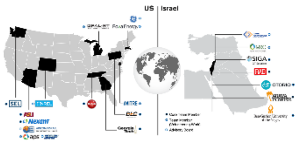
Technical Content: Continual Forecasting with Sparse System Updates

$$\frac{dN}{dt} = I - f(t)NP - qN,$$
$$\frac{dP}{dt} = f(t)NP - P,$$

A driven ecosystem: Annual blooms of phytoplankton under seasonal driving



Product: A Working Manuscript to be Submitted Shortly



Digital twins of nonlinear dynamical systems

Ling-Wei Kong,[1] Yang Weng,[1] Bryan Glaz,[2] Mulugeta Haile,[2] and Ying-Cheng Lai[1,3,*]

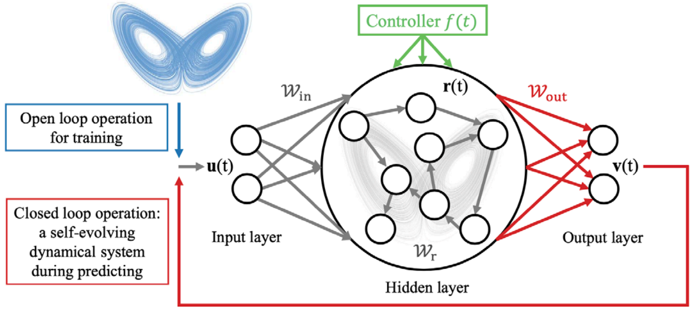
[1] *School of Electrical, Computer and Energy Engineering, Arizona State University, Tempe, Arizona 85287, USA*

[2] *Vehicle Technology Directorate, CCDC Army Research Laboratory, 2800 Powder Mill Road, Adelphi, MD 20783-1138, USA*

[3] *Department of Physics, Arizona State University, Tempe, Arizona 85287, USA*

(Dated: May 3, 2022)

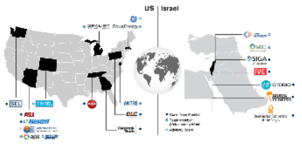
We articulate the design imperatives for creating machine-learning based digital twins for nonlinear dynamical systems subject to external driving, which can be used to monitor the "health" of the target system and to anticipate its possible future collapse in different scenarios. The digital twins are tested on prototypical systems from optics, ecology, and climate, where the respective specific examples are a driven chaotic CO_2 laser system, a model of phytoplankton subject to seasonality, and the driven Lorenz-96 climate network. We demonstrate that, with a single or parallel reservoir computers as the platform, the digital twins are capable of a variety of challenging forecasting and monitoring tasks. In particular, a digital twin created according to our design imperatives has the following capabilities: (1) extrapolating the dynamics of the target system to parameter regimes that it has never experienced before, (2) making continual forecasting and monitoring with sparse real-time updates under nonstationary external driving, (3) inferring the existence of hidden variables in the target system and accurately reproducing/predicting their dynamical evolution into the future, (4) adapting to external driving of different waveforms, and (5) extrapolating the global bifurcation behaviors to network systems of different sizes. These features make our digital twins appealing in significant applications such as monitoring the health of critical systems of current interest and forecasting their potential collapse induced by environmental changes or perturbations. Such systems can be an infrastructure, an ecosystem, or a regional climate system.



ACKNOWLEDGMENT

This work was mainly supported by U.S.-Israel Energy Center managed by the Israel-U.S. Binational Industrial Research and Development (BIRD) Foundation.

Commercialization Plan



Past encounter with commercialization (Lai):

- In August 2020, the Air Force/MIT Artificial Intelligence Accelerator launched a public challenge to help create the artificial intelligence needed to solve the magnetic navigation problem.
- The specific call was for the signal enhancement for magnetic navigation (MagNav) challenge problem with the goal to use magnetometer readings recorded from within a cockpit and remove the aircraft magnetic noise to yield a clean magnetic signal.
- The ASU team led by Lai responded and tested three types of machine learning methods: multilayer perceptrons (MLPs), reservoir computing, and long short-term memory (LSTM) neural networks.
- In December 2020, the Air Force/MIT Artificial Intelligence Accelerator placed the ASU team as the winning team.
- The involved Air Force officers suggested to Lai to commercialize the machine-learning technique.

The ASU Task 11 team will work with Nexant to incorporate the principle and methodologies of digital twins for AI-based intrusion detection into the existing industrial Operational Technology and Industrial Control Systems management software tools.