C3.ai Digital Transformation Institute

ANNUAL REPORT 2021-2022

The C3.ai Digital Transformation Institute is a research consortium dedicated to accelerating the benefits of artificial intelligence for business, government, and society. The Institute engages the world's leading scientists to conduct research and train practitioners in the new science of digital transformation, which operates at the intersection of artificial intelligence, machine learning, cloud computing, internet of things, big data analytics, organizational behavior, public policy, and ethics.

TABLE OF CONTENTS

The National Energy Research Scientific Computing Center at Lawrence Berkeley National Laboratory.

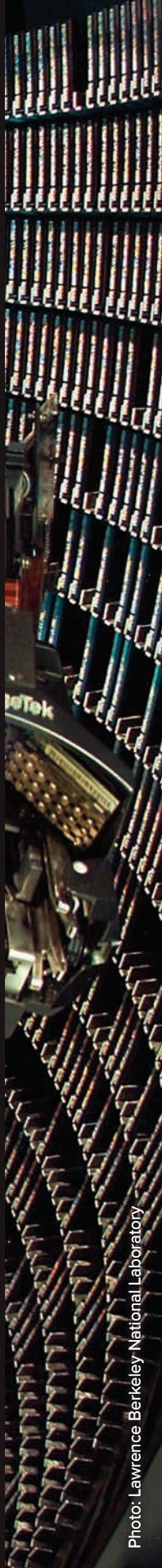


Photo: Lawrence Berkeley National Laboratory

TRANSFORMATIVE TIMES

When the C3.ai Digital Transformation Institute issued its third call for proposals for AI research to transform cybersecurity and secure critical infrastructure last December, few imagined the increased attention that cybersecurity would command when it came time to announce awards for selected proposals this past March, amid heightened global tensions.

The cybersecurity awards were announced at the Institute's second annual research symposium in Miami – also its first-ever in-person event of any kind. C3.ai DTI was launched two years earlier, in March 2020, just as the world entered a lockdown because of COVID-19.

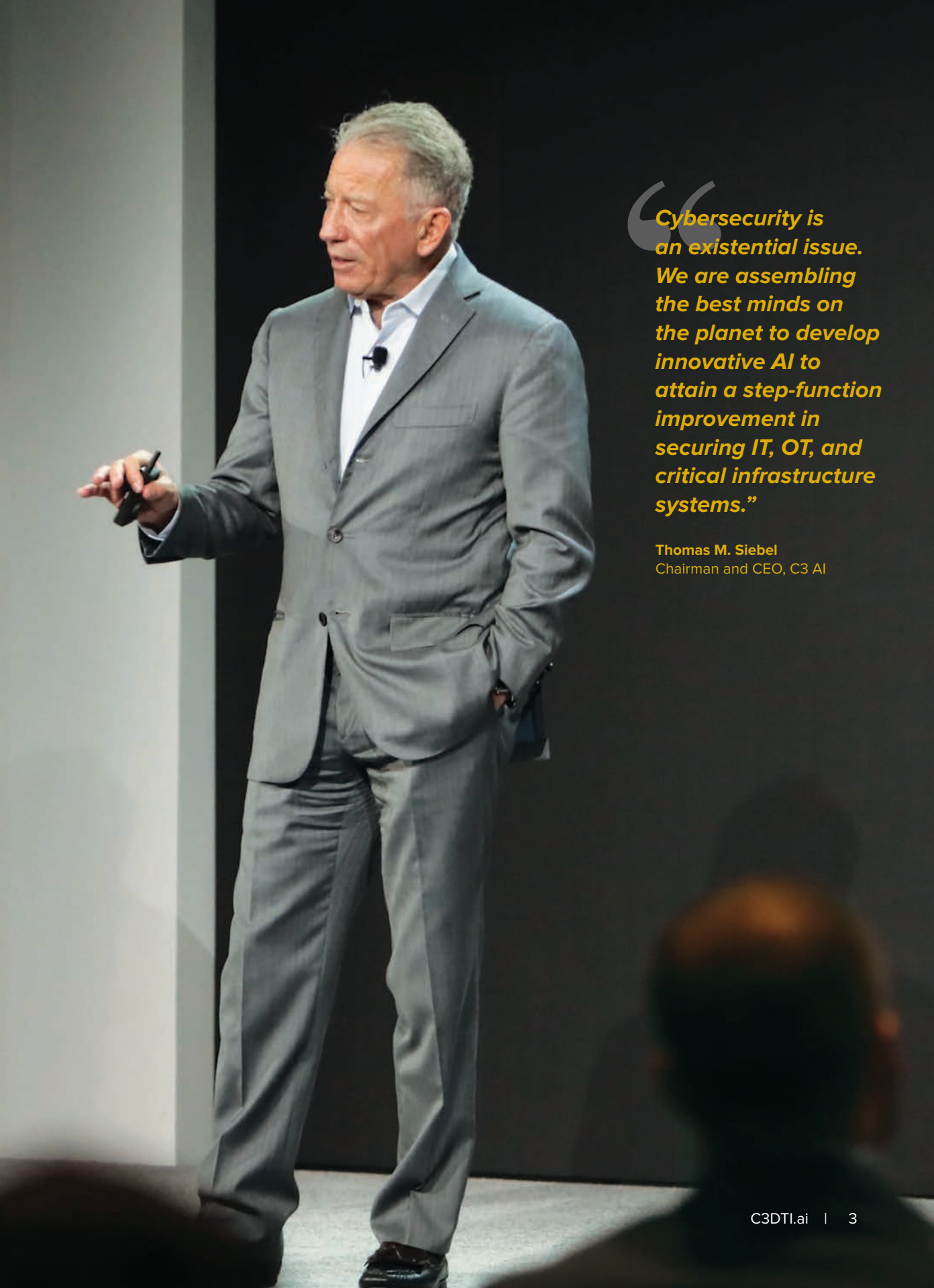
At that time, we issued the first call for proposals for AI research to mitigate COVID-19 and future pandemics. As it turns out, that research reaches far beyond pandemics – AI-driven advances in medical imaging, drug discovery, "virtual physical exams," a clinical care "GPS," and the like have the potential to fundamentally change how medicine operates.

The second call in 2021 was for AI research for energy and climate security. While we all recognize the clear and present danger of climate change, fewer would have predicted how the urgency of transitioning away from fossil fuels would skyrocket after Russia invaded Ukraine. We expect these projects to have outsize impact as well.

To witness these massive upheavals, in face-to-face discussions with the foremost scientific minds on the planet, was to truly take in this historic inflection point. It called to mind the thesis of my book on Digital Transformation: how rapid upheaval creates economic disruption, how organizations need to reinvent the way they interact with the changing world. How they must recognize when an existing model has run its course, and evolve.

As the groundbreaking science within these pages describe, the C3.ai DTI is at the forefront of advancing foundational methods and tools that will provide impactful solutions to pressing, societal-scale issues.

– Thomas M. Siebel



Cybersecurity is an existential issue. We are assembling the best minds on the planet to develop innovative AI to attain a step-function improvement in securing IT, OT, and critical infrastructure systems."

Thomas M. Siebel
Chairman and CEO, C3 AI

LEADERSHIP

The C3.ai Digital Transformation Institute was established in spring 2020 by C3 AI, Microsoft Corporation, the University of California, Berkeley, and the University of Illinois at Urbana-Champaign. Institute partners include Carnegie Mellon University, KTH Royal Institute of Technology, Massachusetts Institute of Technology, Princeton University, Stanford University, University of Chicago, Lawrence Berkeley National Laboratory, and the National Center for Supercomputing Applications at the University of Illinois at Urbana-Champaign. The Institute is jointly managed and hosted by the University of California, Berkeley and the University of Illinois at Urbana-Champaign.

ADVISORY BOARD

Thomas M. Siebel
Chairman and CEO, C3 AI

Eric Horvitz
Chief Scientific Officer, Microsoft

S. Shankar Sastry
Co-Director, C3.ai DTI

Thomas M. Siebel Professor of Computer Science

R. Srikant
Co-Director, C3.ai DTI

Fredric G. and Elizabeth H. Nearing Endowed Professor of Electrical and Computer Engineering

EXECUTIVE COMMITTEE

Jonathan Carter
Campus Lead, C3.ai DTI
Associate Lab Director for
Computing Sciences
Lawrence Berkeley National Laboratory

Michael Franklin
Campus Lead, C3.ai DTI
Liew Family Chairman of
Computer Science
University of Chicago

Karl H. Johansson
Campus Lead, C3.ai DTI
VR Distinguished Professor of Electrical
Engineering and Computer Science
KTH Royal Institute of Technology

Christopher Manning
Campus Lead, C3.ai DTI
Thomas M. Siebel Professor of
Machine Learning
Stanford University

Asuman Ozdaglar
Campus Lead, C3.ai DTI
MathWorks Professor of Electrical
Engineering and Computer Science
Massachusetts Institute of Technology

H. Vincent Poor
Campus Lead, C3.ai DTI
Michael Henry Strater University
Professor
Princeton University

William Sanders
Campus Lead, C3.ai DTI
Dr. William D. and Nancy W. Strecker
Dean, College of Engineering
Carnegie Mellon University

S. Shankar Sastry
Co-Director, C3.ai DTI
Thomas M. Siebel Professor of
Computer Science
University of California, Berkeley

Costas Spanos
Co-Chief Scientist, C3.ai DTI
Andrew S. Grove Distinguished
Professor of Electrical Engineering
and Computer Sciences
University of California, Berkeley

R. Srikant
Co-Director, C3.ai DTI
Fredric G. and Elizabeth H. Nearing
Endowed Professor of Electrical
and Computer Engineering
University of Illinois at Urbana-
Champaign

Tandy Warnow
Co-Chief Scientist, C3.ai DTI
Grainger Distinguished Chair
of Engineering
University of Illinois at Urbana-
Champaign

PARTNER INSTITUTIONS

The C3.ai Digital Transformation Institute consortium includes members from academia, national laboratories, and industry. The Industry Partners program enables leading companies from around the world to engage with C3.ai DTI researchers and activities. Industry partners are also encouraged to collaborate on research projects, participate in the annual C3.ai DTI Research Symposium, and attend workshops, colloquia, and other special events.

ACADEMIC PARTNERS

Berkeley
UNIVERSITY OF CALIFORNIA

UNIVERSITY OF ILLINOIS
URBANA-CHAMPAIGN

Carnegie Mellon University

KTH
VETENSKAP
OCH KONST

Massachusetts
Institute of
Technology

PRINCETON
UNIVERSITY

Stanford
University

THE UNIVERSITY OF
CHICAGO

RESEARCH LABORATORIES

BERKELEY LAB

National Center for
Supercomputing Applications
UNIVERSITY OF ILLINOIS URBANA-CHAMPAIGN

INDUSTRY PARTNERS

C3.ai

Microsoft

Baker Hughes

RESEARCH AWARD PROGRAM

The C3.ai Digital Transformation Institute supports teams of the best researchers in the world to advance AI techniques for industrial, commercial, and public sector applications. This rich ecosystem will help address some of the most complex issues inherent in a massive societal digital transformation and build the foundation for a new Science of Digital Transformation. C3.ai DTI annually awards cash grants and access to computing resources for research projects based at consortium universities.

In February 2021, the Institute released its second call for proposals to advance AI for energy and climate security. In June, the institute awarded 22 projects that apply AI/ML for sustainability initiatives, carbon sequestration, advanced energy and carbon markets, cybersecurity of power and energy infrastructure, smart grid analytics, distributed energy resource management, climate change modeling, and improved natural catastrophe risk assessment.

The third call for proposals, for AI to transform cybersecurity and secure critical infrastructure, was released in December 2021. In March 2022, C3.ai DTI awarded 24 projects for AI resilience, anomaly detection, advanced persistent threats, securing cyber-physical infrastructure, forensics, emerging financial infrastructure, vulnerability identification, and insider threats.

AI RESEARCH PROJECTS TO ADVANCE AI FOR ENERGY AND CLIMATE SECURITY

In June 2021, the C3.ai Digital Transformation Institute announced awards from its second call for proposals to advance breakthrough AI research to ensure energy and climate security and lead the way to a lower-carbon, higher-efficiency economy. A total of $4.6 million, along with access to the C3 AI Suite and Microsoft Azure computing and storage, was awarded for 22 research projects now underway.

SUSTAINABILITY

AI-Driven Materials Discovery Framework for Energy-Efficient and Sustainable Electrochemical Separations

Xiao Su
University of Illinois at Urbana-Champaign

Seven hundred million people worldwide lack access to clean water. Standard water purification and treatment methods are highly carbon- and chemical-intensive. Electrically-driven purification offers a powerful alternative that eliminates chemical pollution and integrates well with renewable energy. Using machine learning, molecular dynamics simulations, and first-principles calculations, this team envisions a new paradigm for designing redox-polymers for anion-selective separations. Redox-active polymers are a good target for electrochemical control of ion-selectivity and reversibility, through tailored synthesis. This team expects their proof-of-concept to pave the way to accelerate development of new treatment and remediation technologies with a reduced carbon footprint and enhanced energy efficiency.

Learning in Routing Games for Sustainable Electromobility

Henrik Sandberg
KTH Royal Institute of Technology

The largest contributor to greenhouse gas emissions worldwide, the transportation sector is poised for tremendous change. Electrifying road transportation can defer emissions from roads to electric power generation, yet zero-emission mobility raises new questions. What should new routing strategies look like? How to deploy heavy-duty vehicles at scale and strike a balance between operational costs, sustainability, and power grid constraints? This team is designing next-gen traffic-routing algorithms and tools to fuse various noisy (and often incomplete) data while also accounting for cost, infrastructure deterioration, and environmental externalities.

Eric Horvitz
Chief Scientific Officer, Microsoft

"Since the Industrial Revolution, humans have injected about two trillion metric tons of greenhouse gases into the Earth's atmosphere. About 50 billion metric tons are introduced every year. So it's great to see these high-aspiration projects... We need these kinds of audacious, yet technically sound – and scientifically sound – projects, to be pursued by teams known for deep technical thinking, optimism, and creativity."

AI FOR CARBON SEQUESTRATION

Optimization of Agricultural Management for Soil Carbon Sequestration Using Deep Reinforcement Learning and Large-Scale Simulations

Naira Hovakimyan
University of Illinois at Urbana-Champaign

Two of the most significant challenges currently facing humanity are climate change and food security; this project is designed to address both. Sequestering carbon in cropland soils can be a tradeoff with crop yield, yet, according to this team, an intelligent agricultural management system can maximize both at the same time. Using deep reinforcement learning and large-scale soil and crop simulations, the team is building a simulator modeling complex soil-water-plant-atmosphere interaction. Running on a high-performance computing platform, massive simulations can reveal the effects of various management strategies under many weather and soil conditions to guide policies that maximize both stored organic carbon and crop yield.

AI FOR ADVANCED ENERGY AND CARBON MARKETS

The Role of Interconnectivity and Strategic Behavior in Electric Power System Reliability

Ali Hortacsu
University of Chicago

How can AI keep calamities like the Texas power crisis of 2021 from reoccurring? Combining structural economic estimation and optimization with machine learning, this team is trying to find answers by devising a new method to simulate market outcomes – using electricity market data from the neighboring (and similar) MISO South region and a rich dataset on natural gas pipelines to study interactions between the two systems and ultimately, guide the development of more protective policies.

AI FOR CARBON SEQUESTRATION

Claire Tomlin
University of California, Berkeley

Affordable Gigaton-Scale Carbon Sequestration: Navigating Autonomous Seaweed Growth Platforms by Leveraging Complex Ocean Currents and Machine Learning

Seaweed fixates dissolved CO_2 into biomass that then falls into the deep ocean, confining carbon for millennia. One research team asks, how can this natural process be harnessed to sequester carbon – at gigaton scale? Partnering with a startup, the researchers have prototyped platforms of floating seaweed farms designed to ride the open ocean. Because motorized steering is prohibitively expensive, they envision the platforms "hitchhiking" on ocean currents. With AI-devised control and navigation systems and solar-powered propulsion, the team aims to optimize seaweed growth and steer platforms over deep channels to deposit full loads. The cost per ton of CO_2 sequestered by platforms using currents for navigation would be dramatically lower than other approaches, resulting in affordable gigaton-scale sequestration.

AI FOR FOR ADVANCED ENERGY AND CARBON MARKETS

Kaiyu Guan
University of Illinois at Urbana-Champaign

Carbon Credit Over U.S. Midwestern Cropland Using AI-Based Data-Model Fusion

To truly evaluate climate-smart agricultural practices and build market-based agricultural carbon credit markets, you first need accurate, cost-effective carbon credit accounting. By building this foundation for an agricultural carbon market, this project can contribute to climate change mitigation. Using multi-scale AI algorithms and multi-source sensing data (ground, airborne, and satellite), the AI-based data-model fusion system is designed to quantify historic carbon credit over Midwestern cropland and assess carbon credit potentials under different management scenarios at field scale.

CYBERSECURITY OF POWER AND ENERGY INFRASTRUCTURE

Private Cyber-Secure Data-Driven Control of Distributed Energy Resources

Subhonmesh Bose
University of Illinois at Urbana-Champaign

As “prosumers” with distributed energy resources (DERs) become active participants in a vibrant energy economy, they play a different role than traditional consumers. While individual DERs may have a small energy footprint, together they can generate valuable grid services. This team is investigating data-driven distributed control of DERs via multi-agent Reinforcement Learning (MARL), designing algorithms to protect private information and detect data integrity system attacks with multiple, almost-identical subsystems.

Cyberattacks and Anomalies for Power Systems: Defense Mechanism and Grid Fortification via Machine Learning Techniques

Javad Lavaei
University of California, Berkeley

Power systems are dependent on data analytics because major operational problems – such as security-constrained optimal power flow, contingency analysis, and transient stability analysis – rely on knowledge from sensory data. Yet current industry practices tend to work well enough under normal situations but less well under adverse conditions, including cyberattacks. Working at the intersection of power systems, machine learning, and optimization, this team is investigating how to design a set of ML algorithms with mathematical guarantees to detect cyberattacks and anomalies; trade-offs between algorithm accuracy and computational power requirements; and how to fortify the grid to ensure that it is incapable of propagating misinformation in case of a cyberattack.

A Joint ML and Physics-Driven Approach for Cyber-Attack Resilience in Grid Energy Management

Amritanshu Pandey
Carnegie Mellon University

This team has identified a critical gap in the resilience of current Energy Management Systems in light of emerging cyber-attacks, and is combining machine learning with traditional physics-based simulations for scalable solutions. While traditional approaches alone may detect complex attacks, they are impractical (e.g., assuming complete grid knowledge) and slow, while machine learning techniques are fast but may lack the required fidelity to capture anomalies and complex attacks, resulting in high false positives and false negatives. By combining domain knowledge from grid-physics with ML techniques, this project aims to fortify cyber-resilient Energy Management Systems.

SMART GRID ANALYTICS

Scalable Data-Driven Voltage Control of Ultra-Large-Scale Power Networks

Alejandro Dominguez-Garcia
University of Illinois at Urbana-Champaign

Large-scale integration of renewable generation in electric power distribution systems is hampered by increased operational risks outside the acceptable voltage range. Both under- and over-voltage conditions can damage equipment and may even cause wide-scale blackouts. The challenges of regulating voltages include the absence of exact distribution system models and, lacking sensors and adequate communication infrastructure, the difficulty of accurately estimating. This team is developing a scalable, data-driven control strategy without the knowledge of a system model, capable of providing fast and optimal response to under- and over-voltage events in large-scale distribution systems.

LEADING VOICES: ON DIGITAL AGRICULTURE

Soil carbon sequestration has the potential to offset 5 to 15 percent of global fossil-fuel emissions. Yet it is challenging to find the optimal management practices maximizing soil carbon sequestration while improving crop productivity.

We're all familiar with precision medicine; digital agriculture is relatively junior in this sense. Lots of the things that are happening today in this industry are based on past practices, common sense, farmers' experience, and others – so now is the time to revolutionize this industry.

With the opportunities of data collection for so many sensors, aerial imagery with satellite data resolution becoming higher and better, one can truly optimize these practices to get better performance for crop yield, to optimize management, as well as for carbon sequestration.

Early results of nitrogen management studies with corn crops in Iowa and Florida demonstrate that, compared to the baseline, applying nitrogen fertilizers with the trained policy leads to more yield and roughly the same nitrogen leaching. In other words, our optimization leads to better results.

– Naira Hovakimyan, University of Illinois at Urbana-Champaign

DISTRIBUTED ENERGY RESOURCE MANAGEMENT

Minjie Chen
Princeton University

Machine Learning for Power Electronics-enabled Power Systems: A Unified ML Platform for Power Electronics, Power Systems, and Data Science

In the future, clouds of distributed and renewable energy resources will support the grid. These will require grid-tied power electronics to connect these resources. With their dynamic behaviors, these inverters challenge a system's stability and control. This team is building a family of C3 AI-enabled methods for learning, optimization, and stability analysis of grid-tied inverters and power electronics-enabled power systems to develop a unified ML platform for power electronics, power systems, and data science research. As a case study to demonstrate a holistic modeling approach, they plan to model a single inverter first, then a cluster connected as a microgrid.

Offline Reinforcement Learning for Energy-Efficient Power Grids

Sergey Levine
University of California, Berkeley

This team is developing Offline RL algorithms incorporating real-world data for training an RL agent to reduce emissions associated with running an electrical grid. Offline RL allows learning policies entirely from previously collected historical data, without any simulation, while still optimizing to improve metrics above and beyond the historical policy that generated that data. In this case, Offline RL will enable the reduction of emissions using electrical grid data while retaining the benefits of testing in simulation. The team hypothesizes that this approach will learn a more efficient grid management policy that can significantly reduce both emissions and costs of electricity generation.

DISTRIBUTED ENERGY RESOURCE MANAGEMENT

Sharing Mobile Energy Storage: Platforms and Learning Algorithms

Kameshwar Poolla
University of California, Berkeley

In our collective sustainable energy future, electricity storage will be required for diverse services, including efficient electrified transportation systems, zero-emissions balancing of intermittent renewable generation, and ramping service to balance supply and demand when solar PV goes offline. But electricity storage is very expensive and requires high use rates to recoup capital costs. This team proposes a solution: Developing a shared mobile energy storage platform to serve many geographically distributed users, which could provide sufficiently high utilization rates to justify investment costs.

Data-Driven Control and Coordination of Smart Converters for Sustainable Power System Using Deep Reinforcement Learning

Qianwen Xu
KTH Royal Institute of Technology

To address the challenges of voltage instability of all-renewable electric power systems, this team aims to transform current model-based control methods and contingencies with data-driven and communication-efficient control and coordination of smart converters. The team will design and deploy novel algorithms in real experimental microgrids already developed in the KTH lab. "The developed software will add significant value to industry," says P.I. Wu, citing the advanced DRL solutions, active grid management, and grid data analytics tested on real hardware.

AI FOR IMPROVED NATURAL CATASTROPHE RISK ASSESSMENT

Tropical Cyclone Modeling and Enabling the Resilience Paradigm

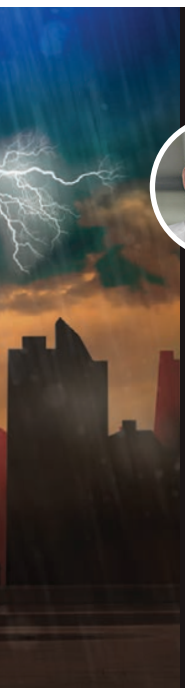
Arindam Banerjee
University of Illinois at Urbana-Champaign

As a changing climate worsens natural catastrophes such as tropical cyclones, wildfires, and floods, these weather events will have a huge impact on infrastructure, lifeline networks, and human life and well-being. To assess natural catastrophe risks and design suitable adaptation measures, this team aims to improve natural catastrophes modeling under a changing climate and develop resilient infrastructure and lifeline networks that can gracefully degrade and quickly recover after disasters – initially targeting tropical cyclone modeling along the U.S. Eastern Seaboard and improving transportation network resilience.

Multi-Scale Analysis for Improved Risk Assessment of Wildfires Facilitated by Data and Computation

Marta Gonzalez
University of California, Berkeley

This team is creating a comprehensive wildfire protection system to guard against catastrophic disasters that threaten lives and critical infrastructure, particularly at the wildland urban interface. The key is targeting strategies, planning, and policies to reduce wildfire intensity and rate of spread. This research aims to better identify and model wildfire risk so that planning and policy can be informed by improved, AI-driven modeling under current and future climate conditions.



RESILIENT ENERGY SYSTEMS

Eytan Modiano
Massachusetts Institute of Technology

A Learning-Based Influence Model Approach to Cascading Failure Prediction

Large blackouts in power grids are often caused by uncontrolled failure cascades. If we could better predict the failure cascade process, we can better protect and secure power systems. Using machine learning, that is exactly this team's goal. They are designing a hybrid learning framework based on the influence model, which is a Markovian-like graphical model that can capture the failure cascade process, and plan to evaluate the learning framework's prediction performance on real systems for accuracy, efficiency, and robustness to load variations.

RESILIENT ENERGY SYSTEMS

Reinforcement Learning for a Resilient Electric Power System

Alberto Sangiovanni-Vincentelli
University of California, Berkeley

As we have unfortunately seen, electric grids are increasingly vulnerable to growing cyber-threats by malicious actors. Physical attacks that lead to system failures are also on the rise. Then there's climate change, with increasingly severe weather and natural disasters harming electric grids. And what if several of these threats are present at once? Using reinforcement learning-based methods, Byzantine game analysis, and adding a human-in-the-loop audit, rare-event modeling, and sequential decision-making, the team's end product will be an open-source application for improving network resilience on large-scale, real-world power networks.

AI FOR IMPROVED CLIMATE CHANGE MODELING

Machine Learning to Reduce Uncertainty in the Effects of Fires on Climate

Hamish Gordon
Carnegie Mellon University

Fires have important but poorly understood effects on climate, dominated by smoke aerosols and interactions with clouds. Improved climate models are needed to predict these effects, but predictions differ widely between models. By collaborating with statisticians to extend existing uncertainty quantification approaches for climate models using advanced machine learning, this team has set out to determine the full impact of fires on Earth's changing climate. New statistical techniques will also help constrain aerosol radiative forcing, and can be further applied to improve uncertainty quantification in other scientific disciplines.

AI FOR IMPROVED CLIMATE CHANGE MODELING

Da Yang
Lawrence Berkeley National Laboratory

Interpretable Machine Learning Models to Improve Forecasting of Extreme-Weather-Causing Tropical Monster Storms

Researchers are developing interpretable, machine-learning models to forecast the Madden-Julian Oscillation — the MJO, "Storm King" of Earth's tropics — an irregular, month-long, planetary-scale rainfall pattern over the Indian and Pacific Oceans. MJO-associated winds and precipitation are felt across the globe — forming hurricanes, initiating El Nino, and producing rainfall and heatwaves in North America. Current Numerical Weather Prediction models use coarse computing grids — inevitably producing coarse forecasts. In March 2015, the most powerful MJO on record triggered an El Nino event, yet forecasts had failed to predict MJO initiation and evolution. This research team aims to improve MJO forecasting by developing a computationally efficient ML model that learns from observations. To address limited observations, researchers will use transfer learning to train a physics-aware convolutional neural network (CNN) – first on model simulations and then on observations. With a skilled CNN, researchers can produce more precise MJO forecasts to provide essential information for strategic flood control and water management.

AI-Based Prediction of Urban Climate and Its Impact on Built Environments

Wei Liu
KTH Royal Institute of Technology

Examining urban climate and its impact on built environments could provide researchers, urban planners, environmental engineers, and decision-makers with critical environmental quality evaluation guidelines and tools that could lead to effective pollutant mitigation strategies. Yet creating such tools has been hampered by computational speed, accuracy, and robustness. AI-based Computational Fluid Dynamics (CFD) simulation might offer a solution. In efficiency, predictions from AI-based models are expected to be at least 10 times faster; for accuracy, within a 10 percent difference from that of conventional CFD simulations.

AI FOR LEAKS AND EMISSIONS DETECTION

Plant-Wide Leak Detection in Liquified Natural Gas Assets

RS Sreenivas
University of Illinois at Urbana-Champaign

Methane is a potent greenhouse gas with greater impact on global warming than carbon dioxide. A 2018 research study shows actual methane emissions from the U.S. oil and natural gas supply chain are about 6 percent higher than EPA estimates, because existing measurement methods commonly miss emissions under abnormal operating conditions. The IEA estimate of current methane emission rates is about 1.7 percent, and Shell aims to bring it down to 0.2 percent by 2025. In an industry partnership with Shell, UIUC researchers are working on an AI/ML and sensor data fusion framework for leak localization and leak estimation using process data. The leak localization algorithm should ideally detect single or multiple leaks and assign suitable probabilities to every potential leak, so that it is an advisory for targeted maintenance to check with additional technologies like acoustic sensing, IR Camera, LIDAR, etc.

LEADING VOICES: ON THE TROPICAL STORM KING

Discovered in the 1970s, the Madden-Julian Oscillation, or MJO – the Tropical Storm King – is a planetary scale rainfall pattern that initiates in the Indian Ocean. When it develops, it grows in amplitude and scale and propagates eastward; the MJO can occupy more than half of the equatorial circumference and last for 30-60 days. Why do we study this?

Most of us live in the mid-latitudes. Personally, I have lived in California for more than a decade. Why do I care about a phenomenon that only happens in the deep tropical atmosphere? That's because I care about how we can accurately forecast extreme weather and flooding events. I cannot stress enough the value that will bring to us. If we focus on the West Coast of the U.S., with or without the MJO, the winter flooding probability is quadrupled.

With a warming climate, the MJO's influence on western U.S. rainfall is increasing. By accurately forecasting, we can potentially anticipate these extreme events with enough lead time to prepare.

– Da Yang, Lawrence Berkeley National Lab

AI RESEARCH PROJECTS TO TRANSFORM CYBERSECURITY AND SECURE CRITICAL INFRASTRUCTURE

In March 2022, the C3.ai Digital Transformation Institute announced 24 awards from its third call for proposals for cybersecurity research projects to harden information security, boost resilience, strengthen anomaly detection, address persistent threats, and identify vulnerabilities and insider threats.

AI RESILIENCE

High Performance Provably Robust AI Methods for Cybersecurity Tasks on Critical Infrastructure

Zico Kolter
Carnegie Mellon University

AI algorithms are known to be vulnerable to subtle, adversarial perturbations to "normal" data to trick an AI algorithm into making large, potentially catastrophic mistakes. In cybersecurity domains, these perturbations risk endangering critical infrastructure with an attack on the AI itself. This project aims to develop new techniques for building AI methods to be high-performance in accuracy and response time and also provably robust against broad categories of adversarial perturbations — with a specific focus on cybersecurity domains. Researchers believe their novel approach allows provably robust models to be trained against semantic threat models, as these can match much more closely to adversarial perturbations that arise in the real world.

Scalable, Secure Machine Learning in the Presence of Adversaries

John Kubiatowicz
University of California, Berkeley

As Machine Learning models grow in size and complexity, training models on very large datasets may require tremendous computing resources. Cloud computing offers a low-cost, scalable approach to training such large, complex models, then used in applications with varying requirements around networking, privacy, latency, etc., pushing ML applications close to the network edge. At the same time, malicious actors attempt to evade or alter an application's ML decision boundaries or engage in Intellectual Property theft and steal models and parameters. This team aims to develop a novel C3 AI Suite plug-in approach to leverage trusted execution hardware to enable robust ML applications to be built, securely trained, and served – preserving user privacy and preventing adversarial extraction of models and their parameters.

REFL: Resilient Distributed Cybersecurity Learning System

Bo Li
University of Illinois at Urbana-Champaign

Federated Learning (FL), an emerging approach to enable scalable intelligence over next-gen AI systems, transforms the ML ecosystem from "centralized over-the-cloud" to "decentralized over-the-local-users" to alleviate communication bottlenecks for pooling massive amounts of data from millions of local users and strengthen user privacy. Yet fundamental challenges remain. First, AI ecosystems decentralized across local users raises the potential of advanced privacy breaches. Second, since it is difficult to verify numerous local user identities, adversarial attacks may occur during training and testing. This project aims to address these security and privacy challenges and enable scalable and secure intelligence for distributed cybersecurity systems to answer critical challenges: how to ensure resilience and security of the distributed systems against training-time and test-time attacks; and how to ensure privacy for local users in the distributed setting.

Fundamental Limits on the Robustness of Supervised Machine Learning Algorithms

Ben Zhao
University of Chicago

Researchers are developing a framework to obtain lower bounds on robustness for any supervised learning algorithm (classifier) when the data distribution and adversary are specified. The framework will work with a general class of distributions and adversaries and can be extended to get lower bounds on robustness for any pre-trained feature extractor or family of classifiers and for multiple attackers operating in tandem. The impact of training and deploying such novel models includes enabling algorithm designers to get a robustness score for either a specific classifier or a family of classifiers. For any adversary, they can compute this score as the gap to optimal performance possible; optimal performance is the equilibrium of a classification game between adversary and classifiers.

ANOMALY DETECTION

Nick Feamster
University of Chicago

Continuously and Automatically Discovering and Remediating Internet-Facing Security Vulnerabilities

The project has two themes: (1) Developing and applying fingerprinting tools and techniques to automatically generate fingerprints for known vulnerabilities and other security weaknesses; and (2) Designing, implementing, and deploying large-scale scanning techniques to uncover these vulnerabilities in a broad array of settings (such as industrial control and other cyber-physical settings). These approaches extend the team's rich body of previous work in both supervised machine learning (to detect, fingerprint, and inventory vulnerable infrastructure), unsupervised machine learning (to detect anomalous device behavior), and large-scale Internet scanning.

ANOMALY DETECTION

AI Techniques for Power Systems under Cyberattacks

Javad Lavaei
University of California, Berkeley

To improve the efficiency, resiliency, and sustainability of power systems and address climate change, power systems operation is becoming data-driven. Data manipulation by malicious actors tampers with grid operation, with catastrophic consequences. Developing frameworks and methodologies that help power operators protect the U.S. power grid against such malicious attacks is of utmost importance to national security. This team will undertake these five objectives: (1) designing graph neural networks to process power data to learn the system's state and detect cyberattacks; (2) developing AI algorithms to detect denial of view and image replays resulting from cyberattacks; (3) developing optimization techniques to robustify neural networks against adversarial data; (4) and (5), developing attack-aware AI methods via distributionally robust optimization and cascading failure analysis.

Physics-Aware AI-Based Approach for Cyber Intrusion Detection in Substation Automation Systems

Alberto Sangiovanni-Vincentelli
University of California, Berkeley

With the integration of information and communications technology and intelligent electric devices, substation automation systems (SAS) greatly boost the efficiency of power system monitoring and control. Yet, at the frontier of wide-area monitoring and control infrastructure of bulk power systems, substations with new vulnerabilities are targets for attackers. To defend against substation cyberattacks, researchers are developing multiple-use-inspired AI innovations that leverage concurrent capabilities of SAS to transform cybersecurity of power systems, including: (1) a framework that synergizes optimization-based attack modeling with inverse reinforcement learning for multi-stage attack detection; (2) a decision-focused distributed CPS modeling approach; and (3) a mathematical program with equilibrium constraints framework of adversarial unlearning for spoofing detection.

ADVANCED PERSISTENT THREATS

Alexandre M. Bayen
University of California, Berkeley

Deep-Learning Detection Algorithms for Advanced Persistent Attacks in Mixed-Autonomy Traffic: Design and Experimental Validation

This project examines the design, deployment, and experimental testing of AI/ML techniques for detecting malicious actors within multi-agent systems – as applied to mixed-autonomy traffic, with a focus on stealthy, advanced, persistent attacks. Over one year in Nashville, Tennessee, researchers will use a next-gen traffic monitoring system known as the I-24 MOTION testbed to generate approximately 200,000,000 vehicle miles of trajectory data processed through the C3 AI platform. The team will control and "pseudo attack" traffic flow on Interstate 24 for a full week, with 100 level-2 self-driving vehicles capable of (safely) influencing the traffic of regular motorists. Researchers aim to demonstrate the ability to detect "attacking" vehicles through the C3 AI Suite implementation of their detection algorithms on the I-24 MOTION system.

ADVANCED PERSISTENT THREATS

AI Support for Cybersecurity

David Wagner
University of California, Berkeley

This team will develop AI methods for detecting cyberthreats and attacks on computer systems and new AI foundations to support cybersecurity. The breakthroughs in machine learning over the past decade provide a great opportunity to put these to work to defend computer systems and critical infrastructure and create a need for new methods that enable organizations to collaborate to detect attacks and protect their data. Researchers will advance these areas, through a team that melds expertise in computer security and AI.

SECURING CRITICAL CYBER-PHYSICAL INFRASTRUCTURE

Cyber Safety Cage for Networks

Cyrille Valentin Artho
KTH Royal Institute of Technology

Industrial robots usually operate within a "safety cage" to ensure that workers are not harmed by a robot in operation. We need the same type of security, simple and explainable, for IT systems. Novel mechanisms that can be embedded in the network are the enabling technology for this type of security at network level. This team proposes a solution using machine learning and test generation – and focusing on explainable AI in their safety cage, so the cage itself can be inspected and validated, along with its effects on network traffic. Machine learning will devise behavioral models with roots in formal modeling to be inherently readable by humans. Test-case generation will validate diverse traces against the model and also showcase potential malicious behavior, validating both positive and negative outcomes.

LEADING VOICES: ON ENCAPSULATING DATA

Everything we're building is built on top of a research project we have called Fog Robotics. In the Fog Robotics environment, we've created a standardized way of communicating data and code – by encapsulating data and code in what we call 'data capsules.' A data capsule is like a shipping container.

The development of shipping containers revolutionized commercial shipping. With a standardized container format, 22 feet or 44 feet, you could put in goods and transport them, and the entire industry was designed around this uniform-sized container – from railroad cars to cranes to ships themselves.

That's what we've done. We put code and data into our 'shipping containers,' encrypt it, and seal it, just like you would seal a shipping container, and we can transport it around the globe.

With the C3 AI Suite, this innovation could move applications, code, models, and model parameters around securely, and users can compute securely within this encrypted environment. Developers of new algorithms could put them into capsules, offer them for sale, and know they can only be operated on in these secure environments, so they don't have to worry about their algorithms leaking.

– Anthony Joseph, University of California, Berkeley

SECURING CRITICAL CYBER-PHYSICAL INFRASTRUCTURE

Nikita Borisov
University of Illinois at Urbana-Champaign

Security for Large-Scale Infrastructure Using Probabilistic Programming

Probabilistic programming allows program writers to specify probabilistic models and estimate distribution parameters based on observations. With AI techniques, it can handle models too complex for direct mathematical analysis. Through three central thrusts, this project looks to probabilistic programming to secure critical infrastructure. Thrust 1: Applying probabilistic programming to generating benign and malicious communications traffic for power grids; managing congestion in computer networks; and using physics models in robust cyber-physical systems. Thrust 2: Studying threats of adversarial inputs to probabilistic programming in the context of applications above; defining realistic threat models and exploring attack strategies. Thrust 3: Designing countermeasures to adversarial input by detecting corrupt inputs and securing machine learning models. The team will use its system for program analysis and transformation to implement automatic robustification of probabilistic programs.

A Compositional Neural Certificate Framework for Securing Critical Networked Infrastructure

Chuchu Fan
Massachusetts Institute of Technology

Security and robustness are increasingly challenging with interconnected modern infrastructures using AI to make decisions. Any mistake in communication or operation could lead to serious consequences. This project aims to understand how to use rigorous methods based on mathematical analysis to overcome the issue that AI-based methods are not certifiably secure and correct. Researchers aim to advance techniques to make full use of the machinery of machine learning and rigorous methods on critical networked infrastructure systems; and develop a framework of algorithms, theories, and software tools to be tested on large critical infrastructures, including connected vehicles, air transportation systems, and power grids.

Democratizing AI-Driven Security Workflows for Critical Energy Infrastructure

Vyas Sekar
Carnegie Mellon University

Critical infrastructure operators constrained by resources and personnel may not have access to such hyperscale IT infrastructures as global-scale visibility, sophisticated DevOps security workflows, and costly bespoke solutions. This research team believes that AI- and ML-driven workflows can help “level the playing field” for critical energy infrastructure operators by helping automate security-relevant workflows and provide early detection of novel threats. Researchers envision an open novel software-defined collaborative AI/ML cybersecurity stack to tackle these challenges and help democratize benefits of AI/ML driven automation for security infrastructures.

Semantic Adversarial Analysis for Secure Critical Infrastructure

Sanjit A. Seshia
University of California, Berkeley

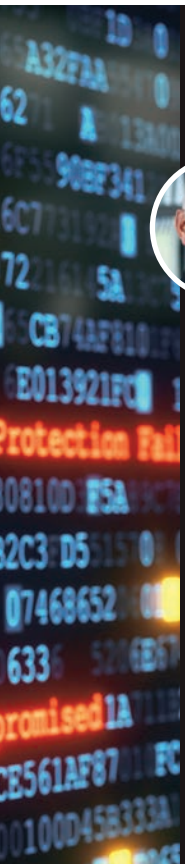
This project is designed to address a pressing need to develop ML methods that find vulnerabilities that matter in the context of the overall system, its specification, and operating environment, not just at the component level. This team is developing such semantic adversarial analysis techniques to find such vulnerabilities. The aim is to enable verification-guided design of ML components, such as deep neural networks to guarantee desired specification, along with run-time monitoring and assured operation in the field.

FORENSICS

Causal Reasoning for Real-Time Attack Identification in Cyber-Physical Systems

György Dán
KTH Royal Institute of Technology

With extensive expertise in cyber-physical systems security, smart grids, and anomaly detection, researchers aim to address questions including how to achieve real-time situational awareness in complex IT infrastructures, how to develop anomaly detectors with low false-positive and low false-negative rates, and, how to use information about IT infrastructure to improve attack identification. The team is aiming for their key contribution to be a succinct representation of the security state of the IT infrastructure, one that allows computationally efficient belief updates in real time and can jointly account for the evolution of the state of the physical system, communication protocols, and infrastructure for accurate detection of attacks and identification – through causal reasoning based on learnt dependency models.



FORENSICS

H. Vincent Poor
Princeton University

Statistical Learning Theory and Graph Neural Networks for Identifying Attack Sources

This project aims to develop new theoretical and algorithmic AI tools to locate attack sources with high accuracy, low computational complexity, and low sample complexity. It has two mutually reinforcing research thrusts: (1) design theoretical tools based on statistical learning, graph theory, and stochastic processes to understand fundamental limits of source localization and to derive important features and structural properties for source localization; and (2) design novel AI algorithms based on graph neural networks and guided by theories in Thrust 1 to locate attack sources quickly and accurately. The team will measure the project's success by the impact of the fundamental results and the accuracy, scalability, and efficiency of algorithms/software toolkits.

Robust and Scalable Forensics for Deep Neural Networks

Ben Zhao
University of Chicago

This team plans to build forensic tools to boost the security of deployed ML systems using post-attack analysis to identify key factors leading to a successful attack. They consider two broad types: “poison” attacks, where corrupted training data embeds misbehaviors into a model during training, and “inference-time” attacks, where an input is augmented by a model-specific adversarial perturbation. For poison attacks, they propose two methods to identify the training data responsible for the misbehavior, one using selective unlearning and one using computation of the Shapley value from game theory. For inference time attacks, they explore use of hidden labels to shift feature representations, making it possible to identify the source model of an adversarial example. Their goal is a principled understanding of these approaches and a suite of usable software tools.

SECURING EMERGING FINANCIAL INFRASTRUCTURE

Blockchain Forensics

Pramod Viswanath
University of Illinois at Urbana-Champaign

A key missing component in blockchain design is the development of disincentives to deviating from prescribed protocol behavior: the same permission-free access blockchains provide to participants also engenders deviant (and malicious) behavior. This blockchain forensics project will study fundamental limits and associated protocols of attributing identity to malicious actors, with cryptographic integrity to the extent possible, and be conducted in the context of blockchain protocols and blockchain applications. The team aims to characterize forensic support of BFT protocols underlying five major central bank digital currency (CBDC) initiatives. The team will also examine Non-Fungible Token (NFT) marketplaces to identify both malicious trades (e.g., wash trades) and attribute malicious actions. The research features novel ML that combines cryptographic traces and protocol specifications with data transcripts.

SECURING EMERGING FINANCIAL INFRASTRUCTURE

Dawn Song
University of California, Berkeley

An Intelligence Platform for Better Security in Decentralized Finance

With the development of blockchain technology, decentralized finance (DeFi) has become an important player in the economy, attracting hundreds of billions of dollars and enabling new financial applications. DeFi has also attracted huge attacks – nearly $1B in financial loss in 2021 alone. This team will design and develop new techniques combining ML and security to build the first DeFi Intelligence Platform, an advanced security infrastructure to strengthen security in the fast-growing DeFi ecosystem.

VULNERABILITY IDENTIFICATION

GAN-Aided Automatic Test Case Generation

Giulia Fanti
Carnegie Mellon University

Software vulnerabilities in libraries and external modules are a leading enabler of cybersecurity attacks. Identifying such vulnerabilities remains massively challenging. While automated testing tools have been widely adopted, they require input test cases to be effective. Crafting a representative and complete set of test cases (especially while respecting constraints imposed by a compiler), remains computationally infeasible. This team will develop novel ML-based techniques for generating inputs for API testing – specifically, the use of generative models to produce valid and useful inputs. They aim to examine novel architectures and training procedures to favor high coverage. Their approach will be evaluated on two use cases – a persistent key-value storage system and Rust Library APIs.

Machine Learning for JavaScript Vulnerability Detection

Corina Pasareanu
Carnegie Mellon University

This team proposes developing the foundations for a unified infrastructure combining machine learning and program analysis for identifying vulnerabilities in JavaScript programs. They aim to achieve low false-negative and false-positive rates and low overhead. Tasks include: (1) Machine Learning, building predictive models for fast, precise, and scalable vulnerability detection in JavaScript programs. (2) Program analysis, complementing existing program analysis tools with improved dynamic techniques for identifying vulnerabilities in JavaScript programs. (3) Integration and evaluation, integrating ML-based and program analysis tools to achieve better accuracy and lower overhead. Researchers will evaluate the performance and effectiveness of this integrated approach with deployed web applications and real Node.js packages.

LEADING VOICES: ON INFRASTRUCTURE CERTIFICATION

In the aviation domain, everything that is allowed to fly has to go through a very rigorous certification procedure to make sure that every component, as well as the whole system, passes through a check. We want to apply the same thing to infrastructure, to help infrastructure designers pass through the certification procedure.

We want our technology to help go through what's called 'failure detection, isolation, and recovery.' Basically, to make a really strong 'bubble' around the system to make sure we can tell a malicious attack from normal signals and trace the signal back to where it's from.

If there's anything that's going to go wrong – an external attack or external noise that's dragging the system away from the desired state – can we recover that? If not, can we isolate that part, and ask a human operator to fix it? This is what our technology is about.

The broader challenge is to guarantee the safety and performance of very large-scale systems, like power grids, or smart cities, with tens of thousands of aircraft delivering goods and people. This is ultimately what our approach is hoping to achieve.

– Chuchu Fan, Massachusetts Institute of Technology

INSIDER THREATS

Protecting Critical Infrastructures Against Evolving Insider Threats

Carl Gunter
University of Illinois at Urbana-Champaign

This project aims to advance machine learning techniques for the detection of insider attacks. The detection system learns patterns and aims to predict events in which trusted insiders violate their trust. The project includes three thrusts: (1) Re-learning, where researchers develop strategies to determine how frequently patterns of behavior should be learned; the key goal here is to learn for long enough to recognize key patterns but not so long that information for the detector becomes obsolete; (2) understanding whether and how insiders may poison training-time data or evade testing-time data to trick a detector into falsely labeling a given target access as legitimate; (3) developing domain knowledge and using it to improve detection systems to reduce false positives. The team will first develop foundations for these three thrusts, then study how they can be integrated and used at scale.

AI-Supported Nudging for Cyber-Hygiene

Cedric Langbort
University of Illinois at Urbana-Champaign

Social engineering attacks that exploit vulnerabilities in human behavior to infiltrate systems are a growing threat to global cybersecurity as large populations of new users in developing countries enter the social media and technology market. Nudges (i.e., "soft influencing" interventions, as opposed to mandates or monetary incentives) may induce desirable online behaviors, but principled design of cyber-hygiene nudges at scale is hampered by a lack of data on nudge efficacy across contexts and available modalities to implement those nudges. This team aims to fill these gaps by addressing: (1) the dearth of data on social engineering threats and cyber-hygiene-related behaviors, especially in developing countries; and (2) the control-theoretic design of nudges, using ML-generated models as a key enabling link between the two.

INSIDER THREATS

Jingrui He
University of Illinois at Urbana-Champaign

Multi-Facet Rare Event Modeling of Adaptive Insider Threats

This team has identified three major challenges when modeling insider threats – the Rarity challenge, Multi-modality challenge, and Adaptivity challenge. The PIs propose multi-facet rare event modeling of adaptive insider threats via novel AI models and algorithms. The work will be carried out through two major research thrusts: (1) Detection of Multi-facet Insider Threats; and (2) Modeling of Adaptive Insider Threats. If successful, these techniques will advance the state-of-the-art of insider threat detection and other related areas – such as outlier detection, rare category analysis, multi-view learning, and adversarial learning.

C3.ai Digital Transformation Institute Annual Research Symposium 2022

The annual C3.ai Digital Transformation Institute Research Symposium brings together research leaders and industry practitioners from around the globe who are working in the new science of digital transformation. The 2022 symposium highlighted C3.ai DTI's impact in enabling foundational digital transformation research at scale through its consortium of world-class research teams. Talks focused on the results of DTI-funded research projects and ongoing research that promises to significantly advance digital transformation science.

FEATURED SPEAKERS

Lt. Gen. Charles L. Moore, Jr.
Deputy Commander
United States Cyber Command

Anup Sharma
Senior Vice President
Global Business Services
LyondellBasell

Detlef Hohl
Chief Scientist
Computation and Data Science
Shell

Garry Kasparov
World Chess Champion and Chairman
Human Rights Foundation

Thomas M. Siebel
Chairman and Chief Executive Officer
C3 AI

Continued on next page.

PROGRAM | DAY 1: MARCH 23

Welcome and Opening Remarks

S. Shankar Sastry, Co-Director, C3.ai DTI, University of California, Berkeley

R. Srikant, Co-Director, C3.ai DTI, University of Illinois at Urbana-Champaign

Keynote

"Defending Forward: A Proactive Posture for Building U.S. Cyber Resiliency"
Lt. Gen. Charles L. Moore Jr., Deputy Commander, United States Cyber Command

DTI Research Talks

Digital Transformation and AI for Energy and Climate Security

Keynote

"The Energy Industry in the Energy Transition: The Role of Digital Innovation, AI, and Academic Collaborations"
Detlef Hohl, Chief Scientist, Computation and Data Science, Shell

Panel Discussion

Digital Transformation and AI for Energy and Climate Security
Hosted by Costas Spanos, Co-Chief Scientist, C3.ai DTI, University of California, Berkeley

DTI Research Talks

Digital Transformation and AI for Energy and Climate Security

Industry Partner Perspective on Cybersecurity

Thomas M. Siebel, Chairman and Chief Executive Officer, C3 AI; Anup Sharma, Senior Vice President, Global Business Services, LyondellBasell

Poster Exposition

PROGRAM | DAY 2: MARCH 24

Keynote

"The Great Game: Coming Out on Top in Chess and Cybersecurity"
Garry Kasparov, World Chess Champion and Chairman, Human Rights Foundation

Awards Announcement

Digital Transformation and AI to Transform Cybersecurity and Secure Critical Infrastructure
S. Shankar Sastry, Co-Director, C3.ai DTI, University of California, Berkeley

Panel Discussion

Digital Transformation and AI to Transform Cybersecurity and Secure Critical Infrastructure
Hosted by S. Shankar Sastry, Co-Director, C3.ai DTI, University of California, Berkeley

DTI Research Talks

Digital Transformation and AI to Mitigate COVID-19 and Future Pandemics

Panel Discussion

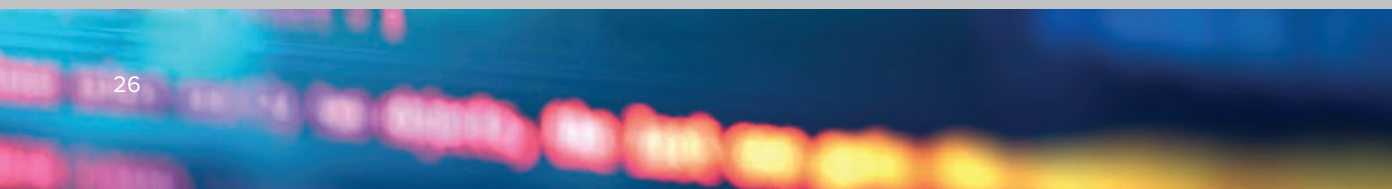
Digital Transformation and AI to Mitigate COVID-19 and Future Pandemics
Hosted by Tandy Warnow, Co-Chief Scientist, C3.ai DTI, University of Illinois at Urbana-Champaign

Closing Remarks

S. Shankar Sastry, Co-Director, C3.ai DTI, University of California, Berkeley
R. Srikant, Co-Director, C3.ai DTI, University of Illinois at Urbana-Champaign

Poster Exposition

See all presentations at:
YouTube.com/C3DigitalTransformationInstitute.



WORKSHOPS ON DIGITAL TRANSFORMATION SCIENCE

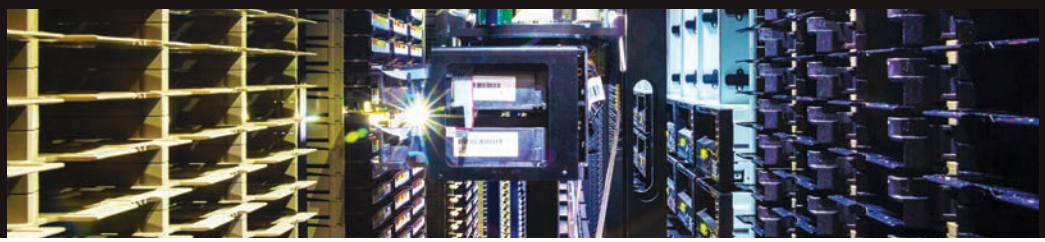


Photo: LBNL, NERSC

The Workshops on Digital Transformation Science are deep dives into foundational topics in digital transformation. These multi-day events are intended for researchers, practitioners, policymakers, and others interested in gaining insights and understanding of topics and trends from leading experts and scientists. Find all workshop videos on the C3.ai DTI YouTube channel at *YouTube.com/C3DigitalTransformationInstitute*.

March 24–26, 2021

DATA-DRIVEN DECISION-MAKING IN SOCIO-TECHNICAL SYSTEMS

Organizers:

Saurabh Amin, Aleksander Madry, and Asu Ozdaglar, Massachusetts Institute of Technology

Abstract:

This workshop explores the confluence of four major elements in large-scale socio-technical systems – machine learning algorithms, platforms, user populations, and regulatory/market structures – in the context of three domains: social media and content moderation, transportation and mobility, and healthcare delivery systems.

Tutorials:

Daily sessions feature three experts diving into one of these domains, addressing such topics as the interaction of algorithms and networks in large-scale social and information systems; control of mixed-autonomy traffic via Deep-RL; and ML for clinical decision-making.

Speakers:

Lars Backstrom, Facebook; Alexandre Bayen, University of California, Berkeley; Marzyeh Ghassemi, University of Toronto; Karl Johansson, KTH Royal Institute of Technology; Matthew Jackson, Stanford University; John Kleinberg, Cornell University; Aleksander Madry, Massachusetts Institute of Technology; Sendhil Mullainathan, University of Chicago; Asu Ozdaglar, Massachusetts Institute of Technology; Shankar Sastry, University of California, Berkeley; Michael Schwarz, Microsoft

June 4, June 11, and June 18, 2021

MACHINE LEARNING FOR A RESILIENT, SECURE, CARBON-FREE ELECTRICITY SUPPLY

Organizers:

Duncan Callaway, University of California, Berkeley; Alejandro Domínguez-García, University of Illinois at Urbana-Champaign; and Marija Ilic, Massachusetts Institute of Technology

Abstract:

Electricity is the lifeblood of our society, and providing a reliable and efficient electricity supply is key to ensuring our welfare and sustainable economic growth. New technologies such as renewable-based generation, Distributed Energy Resources (DERs), and advanced sensors and controls are transforming modern power systems, creating opportunities to increase efficiency and reliability, but also presenting operational challenges. For example, renewables-based generation enables decarbonization, but also increases power supply variability and uncertainty. And increased reliance on advanced sensors and distributed control DER coordination schemes poses cybersecurity and privacy concerns.

Tutorials:

This workshop explored three major domains in power systems — dynamics, control, and protection; cybersecurity and privacy; and markets and optimization — examining areas such as policy optimization, differential privacy, grid graph signal processing, and Deep Reinforcement Learning for Demand Response.

Speakers:

Tamer Başar, University of Illinois at Urbana-Champaign; Spyros Chatzivasileiadis, Technical University of Denmark; Christine Chen, University of British Columbia; Zico Kolter, Carnegie Mellon University; Na Li, Harvard University; Scott Moura, University of California, Berkeley; Ram Rajagopal, Stanford University; Anna Scaglione, Arizona State University; Pascal Van Hentenryck, Georgia Institute of Technology; Louis Wehenkel, University of Liege; Baosen Zhang, University of Washington

August 25-27, 2021

DATA ANALYTICS IN SECURITY AND PRIVACY

Organizers:

Bo Li, University of Illinois at Urbana-Champaign; David Nicol, University of Illinois at Urbana-Champaign; Sean Peisert, Lawrence Berkeley National Laboratory, University of California, Davis

Abstract:

Data science has emerged as a powerful set of tools used to understand and predict the behavior of complex systems. In a cybersecurity context, it is fundamental for applications ranging from analyzing billions of Internet-connected devices for evidence of patched vulnerabilities and ML-based descriptions of normal system behavior to attacks on ML-based models and the learning process itself. This workshop aims for a better understanding of the intersection of data science and cybersecurity and privacy.

Tutorials:

Leaders conducting cutting-edge research, industrial practitioners, and government officials examine areas including end-to-end learning in the data context, dataset biases, what it means to verify neural networks, and cryptography and the democratizing power of learning.

Speakers:

Somesh Jha, University of Wisconsin; George Kesidis, Pennsylvania State University; Zico Kolter, Carnegie Mellon University; Aleksander Madry, Massachusetts Institute of Technology; Patrick Drew McDaniel, Pennsylvania State University; Franzi Roesner, University of Washington; Stefan Savage, University of California, San Diego; Zach Tudor, Idaho National Laboratory; Mayank Varia, Boston University; Ce Zhang, ETH Zurich

September 22-24, 2021

NETWORKS OF MACHINE LEARNING, FOR MACHINE LEARNING, BY MACHINE LEARNING

Organizers:

Manya Ghobadi and Muriel Médard, Massachusetts Institute of Technology

Abstract:

The main driver of new traffic in current backbones has been data shared for Machine Learning. More data has been created in the past five years than in the previous 5,000 years of humanity, and the trend is accelerating. Computation, storage, and communications are no longer interdependent, they are entirely merged. This highly interactive workshop explores this new reality and its technical underpinnings.

Tutorials:

Speakers from industry and academia who are leading these momentous changes will provide perspectives on the present and prospective changes for the future, examining such topics as inclusive search, adventures in learning-based rate control, and model-based Deep Learning and applications to imaging and communications.

Speakers:

Aditya Akella, University of Texas at Austin; Ganesh Ananthanarayanan, Microsoft Research; Pavan Balaji, Facebook; Paolo Costa, Microsoft Research; Yonina Eldar, Weizmann Institute of Science; Nadia Fawaz, Pinterest; Brighten Godfrey, University of Illinois at Urbana-Champaign; H. Vincent Poor, Princeton University; Ariela Zeira, Intel Labs

October 26 & 28, 2021

DIGITAL TRANSFORMATION OF THE BUILT ENVIRONMENT

Organizer:

Costas Spanos, University of California, Berkeley

Abstract:

The built environment is where we spend most of our lives, most of our energy, and where we generate most greenhouse emissions. This impacts our well-being, productivity, and health, as well as the health of the entire ecosystem. With ubiquitous sensing, automation, control, huge data aggregations, and distributed intelligence, digital transformation promises to make the built environment more efficient, healthy, safe, and productive. But new vulnerabilities may surface in this process, such as privacy and inequity across a world of diverse climates, cultures, and socioeconomic conditions.

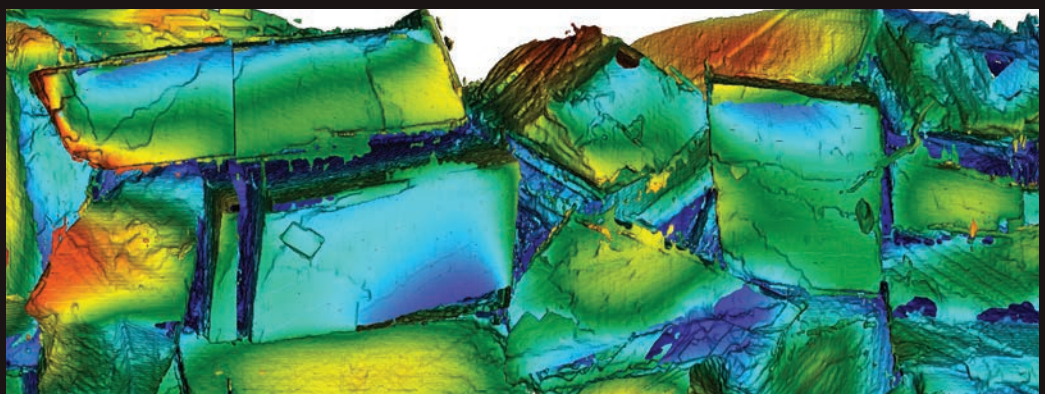
Tutorials:

Facets of transforming the built environment examined include reducing the environmental impact of buildings, using AI to improve energy efficiency in campus buildings, deploying cost-effective AI systems, and examining a novel microgrid model, EcoBlock.

Speakers:

Adrian Chong, National University of Singapore; Alejandro Dominguez-Garcia, University of Illinois at Urbana-Champaign; Carl Gunter, University of Illinois at Urbana-Champaign; Ruoxi Jia, Virginia Tech; Ming Jin, Virginia Tech; Varun Badrinath Krishna, C3 AI; Burt Mayer, C3 AI; Clayton Miller, National University of Singapore; Alberto Sangiovanni-Vincentelli, University of California, Berkeley; Stefano Schiavon, University of California, Berkeley; Sascha von Meier, University of California, Berkeley

COLLOQUIA ON DIGITAL TRANSFORMATION SCIENCE



Data visualization: LBNL, NERSC

The Colloquium on Digital Transformation is a series of weekly online talks on how artificial intelligence, machine learning, and big data can lead to scientific breakthroughs with large-scale societal benefit.

SPRING 2021 SERIES

January 14

A Bayesian Hierarchical Network for Combining Heterogeneous Data Sources in Medical Diagnoses, with Applications to COVID-19

Claire Donnat, University of Chicago

January 28

Modeling and Managing the Spread of COVID-19

Subhonmesh Bose, University of Illinois at Urbana-Champaign

February 4

Triaging of COVID-19 Patients from Audio-Visual Cues

Narendra Ahuja, University of Illinois at Urbana-Champaign

February 18

Why Do ML Models Fail?

Aleksander Madry, Massachusetts Institute of Technology

February 25

Mad Max: Affine Spline Insights into Deep Learning

Richard Baraniuk, Rice University

March 4

Beyond Open-loop Thinking: A Prelude to Learning-Based Intelligent Systems

Lillian Ratliff, University of Washington

March 11

Using Data Science to Understand the Heterogeneity of SARS-COV-2 Transmission and COVID-19 Clinical Presentation in Mexico

Stefano Bertozzi, University of California, Berkeley
Juan Pablo Gutierrez, National Autonomous University of Mexico

March 18

Building Structure into Deep Learning

Zico Kolter, Carnegie Mellon University

April 1

Agent-based Modeling to Understand Social Determinants of Health as Drivers of COVID-19 Epidemics and Test Interventions to Reduce Health Inequities

Anna Hotton, University of Chicago
Jonathan Ozik, Argonne National Laboratory

April 8

Recent Advances in the Analysis of the Implicit Bias of Gradient Descent on Deep Networks

Matus Telgarsky, University of Illinois at Urbana-Champaign

April 15

AI-enabled Deep Mutational Scanning of Interaction between SARS-CoV-2 Spike Protein S and Human ACE2 Receptor

Diwakar Shukla, University of Illinois at Urbana-Champaign

April 22

Is Local Information Enough to Predict an Epidemic?

Christian Borgs, University of California, Berkeley

May 6

Bringing Social Distancing to Light: Architectural Interventions for COVID-19 Containment

Stefana Parascho and Corina Tarnita, Princeton University

May 13

Graceful AI: Backward-Compatibility, Positive-Congruent Training, and the Search for Desirable Behavior of Deep Neural Networks

Stefano Soatto, University of California, Los Angeles

May 20

Feedback Control Perspectives on Learning

Jeff Shamma, University of Illinois at Urbana-Champaign

May 27

AI-Assisted COVID-19 Medical Guidance System Using C3 AI Suite

Lui Sha, University of Illinois at Urbana-Champaign

June 10

Security of Cyber-Physical Systems

P.R. Kumar, Texas A&M University

June 17

Data-Driven Coordination of Distributed Energy Resources

Alejandro D. Dominguez-Garcia, University of Illinois at Urbana-Champaign

June 24

Closing the Loop on Machine Learning: Data Markets, Domain Expertise, and Human Behavior

Roy Dong, University of Illinois at Urbana-Champaign

FALL 2021 SERIES

September 2

A Business Model for Load Control Aggregation to Firm up Renewable Capacity

Shmuel Oren, University of California, Berkeley

September 9

Reinforcement Learning, Bit by Bit

Benjamin Van Roy, Stanford University

September 16

Causal Tensor Estimation

Devavrat Shah, Massachusetts Institute of Technology

September 30

Challenges and Opportunities in Cloud Operations Research

Ishai Menache, Microsoft Research

October 7

Hierarchical Control for Cyber-Physical Systems and Applications to Traffic Management

Murat Arcak, University of California, Berkeley

October 14

Universal Laws and Architectures and Their Fragilities

John Doyle, California Institute of Technology

October 21

Resource Allocation Through Machine Learning in Emerging Wireless Networks: 5G and Beyond to 6G

Sanjay Shakkottai, University of Texas at Austin

October 28

Deep Learning to Replace, Improve, or Aid CFD Analysis in Built Environment Applications

Wei Liu, KTH Royal Institute of Technology

November 18

Toward the Next Era of Traffic Control: From Theory to Applications

Maria Laura Delle Monache, University of California, Berkeley

December 2

Quantifying Carbon Credit Over U.S. Midwestern Cropland Using AI-Based Data-Model Fusion

Kaiyu Guan, University of Illinois at Urbana-Champaign

SPRING 2022 SERIES

February 10

A Fresh Look at Design: A Rigorous Framework for Integrating Model-Based and Data-Based Systems Engineering

John S. Baras, University of Maryland

February 17

On Dynamics-Informed Blending of Machine Learning and Game Theory

Michael I. Jordan, University of California, Berkeley

February 24

Algorithmic Tools for U.S. Congressional Districting: Fairness via Analytics

David Shmoys, Cornell University

March 3

Optimal and Differentially Private Data Acquisition from Strategic Users

Asuman Ozdaglar, Massachusetts Institute of Technology

March 10

How Does the Brain Beget the Mind?

Christos Harilaos Papadimitriou, Columbia University

March 17

Communicating with Anecdotes

Nicole Immorlica, Microsoft Research

March 31

Inducement of Desired Behavior via Soft Policies

Tamer Başar, University of Illinois at Urbana-Champaign

April 7

Online Optimization and Control Using Black-Box Predictions

Adam Wierman, California Institute of Technology

April 14

On Convergence and Stability of Coupled Belief — Strategy Learning Dynamics in Continuous Games

Manxi Wu, University of California, Berkeley

April 21

AI for Social Impact: Results from Deployments for Public Health and Conservation

Miland Tambe, Harvard University

April 28

Allocating Goods, Bads, and Mixed: Fairness and Efficiency through Competitiveness

Ruta Mehta, University of Illinois at Urbana-Champaign

May 5

Auditing and Designing for Equity in Resident Crowdsourcing

Nikhil Garg, Cornell Tech

May 12

Decentralized, Communication-free and Coordination-free Learning in Structured Matching Markets

Chinmay Maheshwari, University of California, Berkeley

SELECT PUBLICATIONS 2021-2022

2021

Easing COVID-19 lockdown measures while protecting the older restricts the deaths to the level of the full lockdown, Scientific Reports, March 12. DTI Co-P.I. Panayotis Kevrekidis.

Evaluation of reopening strategies for educational institutions during COVID-19 through agent-based simulation, Scientific Reports, March 17. DTI P.I. Subhonmesh Bose.

Optimal, near-optimal, and robust epidemic control, Communications Physics, April 20. DTI Co-P.I. Simon Levin.

A Data-Informed Approach for Analysis, Validation, and Identification of COVID-19 Models, IEEEXplore ACC 2021, May. DTI P.I. Prashant Mehta.

Preliminary Immunogenicity of a Pan-COVID-19 T Cell Vaccine in HLA-A*02:01 Mice, bioRxiv, May 5. DTI P.I. David Gifford.

Leveraging A Multiple-Strain Model with Mutations in Analyzing the Spread of Covid-19, IEEEXplore, May 13. DTI P.I. H. Vincent Poor.

Lockdown measures and their impact on single- and two-age-structured epidemic model for the COVID-19 outbreak in Mexico, Math Bioscience, June. DTI P.I. Zoi Rapti.

Online Interactive Platform for COVID-19 Literature Visual Analytics: Platform Development Study, Journal of Medical Internet Research, July 17. DTI P.I. Gerbrand Ceder.

CROP: Certifying Robust Policies for Reinforcement Learning through Functional Smoothing, arXiv, June 17. DTI Co-P.I. Bo Li.

Optimal Testing Strategy for Containing COVID-19: A Case-Study on Indian Migrant Worker Population, IEEE ACC, July 28. DTI P.I. Saurabh Amin.

Reaction-diffusion spatial modeling of COVID-19: Greece and Andalusia as case examples, Physical Review E, August. DTI P.I. Zoi Rapti.

Vaccine nationalism and the dynamics and control of SARS-CoV-2 Science, August 17. DTI Co-P.I. Simon Levin.

Redox-copolymers for the recovery of rare earth elements by electrochemically regenerated ion-exchange, Journal of Materials Chemistry A, August 23. DTI P.I. Xiao Su.

Neighborhoods with the Highest Eviction Filing Rates Have the Lowest Levels of COVID-19 Vaccination, Socius, August 25. DTI Co-P.I. Peter Hepburn.

A pre-registered short-term forecasting study of COVID-19 in Germany and Poland during the second wave, Nature Communications, August 27. DTI P.I. Dimitris Bertsimas.

Classification of COVID-19 from Cough Using Autoregressive Predictive Coding Pretraining and Spectral Data Augmentation, Interspeech, September 3. DTI P.I. Narendra Ahuja.

Conditional Synthetic Data Generation for Robust Machine Learning Applications with Limited Pandemic Data, arXiv, September 14. DTI P.I. Alberto Sangiovanni-Vincentelli.

A Workflow for Offline Model-Free Robotic Reinforcement Learning, ArXiv, September 23, DTI P.I. Lui Sha.

Feedback Particle Filter for Collective Inference, Foundations of Data Science, September. DTI P.I. Prashant Mehta.

Reinforcement Learning with Real-time Docking of 3D Structures to Cover Chemical Space: Mining for Potent SARS-CoV-2 Main Protease Inhibitors, arXiv, October 5. DTI P.I. Teresa Head-Gordon.

Secure Byzantine-Robust Distributed Learning via Clustering, arXiv, October 6. DTI P.I. Oluwasanmi Koyejo.

Clustering Spatial Transcriptomics Data, Bioinformatics, October 8. DTI P.I. Ziv Bar-Joseph.

Medical Imaging of COVID-19, Journal of Medical Imaging, November 3. DTI P.I. Maryellen Giger.

Data-Driven Modeling of Power-Electronics-Based Power System Considering the Operating Point Variation, IEEEXplore ECCE, November 16. DTI P.I. Qianwen Xu.

Machine Learning Methods for Power Flow Control of Multi-Active-Bridge Converters, IEEE COMPEL, December 23. DTI P.I. Minjie Chen.

Deep learning to replace, improve, or aid CFD analysis in built environment applications: A review, Building and Environment, December. DTI P.I. Wei Liu.

Distributed Power System State Estimation Using Graph Convolutional Neural Networks, Semantic Scholar, 2021. DTI P.I. Javad Lavaei.

2022

A Meta-Learning Approach to the Optimal Power Flow Problem Under Topology Reconfigurations, IEEEXplore, January 4. DTI P.I. H. Vincent Poor.

Learning protein fitness models from evolutionary and assay-labeled data, Nature Biotechnology, January 17. DTI P.I. Jennifer Listgarten.

Engineered ACE2 decoy mitigates lung injury and death induced by SARS-CoV-2 variants, Nature Chemical Biology, January 19. DTI P.I. Diwakar Shukla.

Electrochemical remediation of perfluoroalkyl substances from water, Science Direct, January 20. DTI P.I. Xiao Su.

Temporal modelling using single-cell transcriptomics, Nature Reviews Genetics, January 31. DTI P.I. Ziv Bar-Joseph.

Simple Control for Complex Pandemics, IEEEXplore, February 1. DTI P.I. Munther Dahleh.

What Would Jiminy Cricket Do? Towards Agents That Behave Morally, NeurIPS 2021, February 8. DTI Co-P.I. Bo Li.

Rescuing low frequency variants within intra-host viral populations directly from Oxford Nanopore sequencing data, Nature Communications, March 14. DTI Co-P.I. Todd Treangen.

Green Routing Game: Strategic Logistical Planning using Mixed Fleets of ICEVs and EVs, arXiv, April 22. DTI P.I. Henrik Sandberg.

Detection of Covid-19 from Joint Time and Frequency Analysis of Speech, Breathing and Cough Audio, IEEE Xplore, April 27. DTI P.I. Narendra Ahuja.

Maximum *n*-Times Coverage for Vaccine Design, ICLR, May 4. DTI P.I. David Gifford.

Deep learning for CFD analysis in built environment applications: a review, Clima 2022, May 25. DTI P.I. Wei Liu.

Edge Deletion Algorithms for Minimizing Spread in SIR Epidemic Models, SIAM 2022. DTI P.I. Prashant Mehta.

CONTACT

C3.ai Digital Transformation Institute @ Berkeley

University of California, Berkeley
750 Sutardja Dai Hall, MC 1764
Berkeley, California 94720-1764

C3.ai Digital Transformation Institute @ Illinois

University of Illinois at Urbana-Champaign
1205 W. Clark Street, MC-257, Room 1008
Urbana, Illinois 61801

Inquiries and more information

For general inquiries:
info@c3dti.ai

Sign up for DTI newsletter:
C3DTI.ai/contact

C3.ai Digital Transformation Institute

C3DTI.ai

@C3DTI

/C3DTI

/company/c3-ai-digital-transformation-institute

/C3DigitalTransformationInstitute