

# C3.ai Digital Transformation Institute Announces Call for Proposals for AI to Transform Cybersecurity and Secure Critical Infrastructure

December 21, 2021

BERKELEY, Calif. & URBANA, Ill.--(BUSINESS WIRE)-- The [C3.ai Digital Transformation Institute](#) invites scholars, software developers, and researchers to advance the science of digital transformation with artificial intelligence (AI) designed to harden information security (Infosec) and secure critical infrastructure.

"Cybersecurity is an existential issue," said Thomas M. Siebel, Chairman and CEO of C3 AI, a leading enterprise AI software provider. "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."

"Advanced AI and machine learning offer the best opportunity to design robust defensive systems," said C3.ai DTI Co-Director S. Shankar Sastry of UC Berkeley, whose area of research expertise is cybersecurity. "This call for proposals will help design the defenses necessary to securely shield the digital transformation of our economy."

"We aim to develop AI techniques to identify and neutralize malware, ransomware, phishing attacks, and prevent the weaponization of innocent insiders," said C3.ai DTI Co-Director R. Srikant of the University of Illinois at Urbana-Champaign, an expert in AI and networks.

Immediate Call for Proposals: *AI to Transform Cybersecurity and Secure Critical Infrastructure*.

Topics for research awards may include, but are not limited to, the following:

1. AI techniques to identify previously unknown malware, ransomware, and zero-day vulnerabilities, enabling isolation and neutralization
2. AI-enabled network and system crawlers that can continuously search and identify persistent access mechanisms (backdoors), bots, remote access toolkits (RATS), stagers, and Trojans
3. AI forensics and attribution techniques to identify sources of attacks
4. AI techniques to automate simulated adversarial attacks to identify system and network vulnerabilities
5. AI techniques to accurately identify and enable the neutralization of phishing attacks
6. Change management techniques to prevent the weaponization of innocent insiders
7. AI techniques to detect the presence of advanced persistent threats and insider threats
8. AI-enabled network and/or system crawlers that access and continuously evaluate system security levels
9. AI techniques, perhaps in supervised or unsupervised learning, to provide early detection of system and/or network anomalies that might be indicative of unauthorized access, denial of service, or data exfiltration
10. Techniques and methods to enable the development of AI algorithms that are resilient to adversarial attacks
11. AI techniques to identify concentration risk in the software and computer supply chain
12. Change management to transform organizational behavior to manifest best practices in cyber hygiene
13. Techniques to respond to attacks at the organizational and societal level

This third call for proposals is open now, with a submission deadline of **February 7, 2022**. Researchers are invited to learn more about C3.ai DTI and how to submit their proposals for consideration at [C3DTI.ai](#). Award winners will be announced in March 2022, with a start date around June 1, 2022. Award winners may take part in the annual C3.ai DTI Research Symposium, to be held March 22-24, 2022, in Miami, Florida.

Up to USD \$10 million in cash awards will be funded from this third call, ranging from USD \$100,000 to \$1,000,000 each. In addition to cash awards, C3.ai DTI recipients will be provided with significant cloud computing, supercomputing, data access, and AI software resources and technical support provided by Microsoft and C3 AI. This will include unlimited use of the C3 AI® Suite hosted on the Microsoft Azure Cloud, and access to high-performance computing resources at the Lawrence Berkeley National Laboratory and the National Center for Supercomputing Applications (NCSA) at the University of Illinois at Urbana-Champaign. All science developed from C3.ai DTI funded projects accrues to the public domain.

## Establishing the New Science of Digital Transformation

C3.ai DTI focuses its research on AI, machine learning, IoT, big data analytics, human factors, organizational behavior, ethics, and public policy. The Institute supports the development of ML algorithms, data security, and cybersecurity techniques. C3.ai DTI research analyzes new business operation models, develops methods of implementing organizational change management and protecting privacy, and amplifies the dialogue around the ethics and public policy of AI.

## About C3.ai Digital Transformation Institute

[C3.ai Digital Transformation Institute](#) represents an innovative vision to take AI, ML, and big data research in a consortium model to a level that cannot be achieved by any one institution alone. Jointly managed by the University of California, Berkeley and the University of Illinois at Urbana-Champaign, C3.ai DTI attracts the world's leading scientists to join in a coordinated and innovative effort to advance the digital transformation of business, government, and society, and establish the new science of digital transformation. To support the Institute, C3 AI will provide \$57,250,000 in cash contributions over the first five years of operation. C3 AI and Microsoft will contribute an additional \$310 million in-kind, including use of the C3 AI Suite and Microsoft Azure computing, storage, and technical resources to support C3.ai DTI research.

**C3.ai DTI Contact:**

Kap Stann

Communications Manager, C3.ai DTI @ Berkeley

Tel. +1 510-295-9685

[Kstann@berkeley.edu](mailto:Kstann@berkeley.edu)

**Press Contact**

Lisa Kennedy

(415) 914-8336

[pr@c3.ai](mailto:pr@c3.ai)

Source: C3.ai