

PROCEEDINGS OF SPIE

# ***Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications V***

**Latasha Solomon**  
**Peter J. Schwartz**  
*Editors*

**1–4 May 2023**  
**Orlando, Florida, United States**

*Sponsored by*  
SPIE

*Cosponsored by*  
BAE Systems (United States)

*Published by*  
SPIE

**Volume 12538**

Proceedings of SPIE 0277-786X, V. 12538

SPIE is an international society advancing an interdisciplinary approach to the science and application of light.

The papers in this volume were part of the technical conference cited on the cover and title page. Papers were selected and subject to review by the editors and conference program committee. Some conference presentations may not be available for publication. Additional papers and presentation recordings may be available online in the SPIE Digital Library at [SPIDigitalLibrary.org](http://SPIDigitalLibrary.org).

The papers reflect the work and thoughts of the authors and are published herein as submitted. The publisher is not responsible for the validity of the information or for any outcomes resulting from reliance thereon.

Please use the following format to cite material from these proceedings:

Author(s), "Title of Paper," in *Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications V*, edited by Latasha Solomon, Peter J. Schwartz, Proc. of SPIE 12538, Seven-digit Article CID Number (DD/MM/YYYY); (DOI URL).

ISSN: 0277-786X

ISSN: 1996-756X (electronic)

ISBN: 9781510661929

ISBN: 9781510661936 (electronic)

Published by

**SPIE**

P.O. Box 10, Bellingham, Washington 98227-0010 USA

Telephone +1 360 676 3290 (Pacific Time)

[SPIE.org](http://SPIE.org)

Copyright © 2023 Society of Photo-Optical Instrumentation Engineers (SPIE).

Copying of material in this book for internal or personal use, or for the internal or personal use of specific clients, beyond the fair use provisions granted by the U.S. Copyright Law is authorized by SPIE subject to payment of fees. To obtain permission to use and share articles in this volume, visit Copyright Clearance Center at [copyright.com](http://copyright.com). Other copying for republication, resale, advertising or promotion, or any form of systematic or multiple reproduction of any material in this book is prohibited except with permission in writing from the publisher.

Printed in the United States of America by Curran Associates, Inc., under license from SPIE.

Publication of record for individual papers is online in the SPIE Digital Library.

**SPIE. DIGITAL  
LIBRARY**

[SPIDigitalLibrary.org](http://SPIDigitalLibrary.org)

---

**Paper Numbering:** A unique citation identifier (CID) number is assigned to each article in the Proceedings of SPIE at the time of publication. Utilization of CIDs allows articles to be fully citable as soon as they are published online, and connects the same identifier to all online and print versions of the publication. SPIE uses a seven-digit CID article numbering system structured as follows:

- The first five digits correspond to the SPIE volume number.
- The last two digits indicate publication order within the volume using a Base 36 numbering system employing both numerals and letters. These two-number sets start with 00, 01, 02, 03, 04, 05, 06, 07, 08, 09, 0A, 0B ... 0Z, followed by 10-1Z, 20-2Z, etc. The CID Number appears on each page of the manuscript.

# Contents

vii *Conference Committee*

---

## EXPLAINABLE AI AND TRUST

---

- 12538 09 **Explainable AI for trustworthy image analysis** [12538-3]
- 12538 0B **Robust, fair, and trustworthy artificial reasoning systems via quantitative causal learning and explainability** [12538-5]
- 12538 0C **Action clusters: an NLP-powered approach to detecting similarities of actions within battles** [12538-6]

---

## AI VULNERABILITIES AND DEFENSES

---

- 12538 0D **Detection of adversarial attacks on machine learning systems** [12538-7]
- 12538 0E **Autonomous cyber warfare agents: dynamic reinforcement learning for defensive cyber operations** [12538-8]
- 12538 0F **Cyberspace exercises: defending against malicious cyber actors** [12538-9]
- 12538 0G **Command and control with poisoned temporal batch data** [12538-10]
- 12538 0H **Graph representation learning for context-aware network intrusion detection** [12538-11]
- 12538 0I **Adversary decision-making using Markov models** [12538-12]

---

## HUMAN AI TEAMING

---

- 12538 0J **Artificial (military) intelligence: enabling decision dominance through machine learning** [12538-13]
- 12538 0K **Multi-agent playbook for human-robot teaming** [12538-14]
- 12538 0L **Assigning semantic meaning to machine derived competency controlling topics** [12538-15]

- 12538 OM **Joint human and autonomy teaming for defense: status, challenges, and perspectives** [12538-16]
- 12538 ON **Providing predictions of adversary movements in a gridworld environment to a human-machine team improves teaming performance** [12538-17]

---

#### AI-ENABLED C2 AND CONTEXT-AWARE DECISION MAKING

---

- 12538 OO **Toward an adaptive deep reinforcement learning agent for maritime platform defense** [12538-19]

---

#### SPECIAL SESSION ON VIRTUAL, AUGMENTED, AND MIXED REALITY (XR) TECHNOLOGY FOR MDO

---

- 12538 OR **Implementation of a mixed-reality flight simulator: blending real and virtual with a video-see-through head-mounted display** [12538-23]
- 12538 OS **Bringing a colored head-down display symbology heads up: display fidelity review of a low-cost see-through HMD** [12538-24]
- 12538 OT **Seeing through the enemy's eyes (Best Paper Award)** [12538-26]
- 12538 OU **AI on digital twin of facility captured by reality scans** [12538-27]

---

#### FEDERATED/DISTRIBUTED AI/ML

---

- 12538 OV **Tactical agility for AI-enabled multi-domain operations** [12538-28]
- 12538 OW **Semantic vector space mapping in edge of network multi-domain operations** [12538-29]
- 12538 OX **Bayesian Hierarchical convolutional neural networks** [12538-30]
- 12538 OY **Data-efficient, federated learning for raw network traffic detection** [12538-31]
- 12538 OZ **Confident federated learning to tackle label flipped data poisoning attacks (Best Student Paper Award)** [12538-32]
- 12538 IO **Secure federated machine learning for distributed spectrum sensing in communication networks** [12538-33]
- 12538 I1 **Asynchronous federated learning for tactical autonomy** [12538-34]

---

**AI/ML AND RADAR SENSOR TECHNOLOGY: JOINT SESSION WITH CONFERENCES 12535 AND 12538**

---

12538 12 **Adversarial attack on GNN-based SAR image classifier** [12538-36]

---

**SYNTHETIC DATA FOR MULTI-DOMAIN AI/ML APPLICATIONS: JOINT SESSION WITH CONFERENCES 12529 AND 12538**

---

12538 13 **Semi-supervised domain transfer for robust maritime satellite image classification** [12538-37]

---

**AI/ML AND UNMANNED SYSTEMS I: JOINT SESSION WITH CONFERENCES 12538 AND 12549**

---

12538 16 **Delivering on the promise of autonomous agents in the battlefield** [12538-40]

12538 17 **Comparing hand-crafted and learned key-point feature extraction for co-location of sequential low-altitude UAS video frames** [12538-41]

---

**NOVEL AI/ML ALGORITHMS, FRAMEWORKS, AND APPLICATIONS I**

---

12538 19 **Curriculum-heavy reinforcement learning for multi-domain operations** [12538-43]

12538 1B **Reinforcement learning application to satellite constellation sensor tasking** [12538-45]

12538 1C **Hardware accelerators for deep reinforcement learning** [12538-47]

12538 1D **Towards operational resilience for AI-based cyber in multi-domain operations** [12538-68]

---

**NOVEL AI/ML ALGORITHMS, FRAMEWORKS, AND APPLICATIONS II**

---

12538 1E **Results of the airlift challenge: a multi-agent AI planning competition** [12538-48]

12538 1F **Exploiting large neuroimaging datasets to create connectome-constrained approaches for more robust, efficient, and adaptable artificial intelligence** [12538-49]

12538 1G **Modified Hausdorff distance and diffusion equation evolution combined fast manifold Kmeans** [12538-50]

---

**POSTER SESSION**

---

- 12538 1I **Exploring stable diffusion and interpretability of image classification using neural features** [12538-20]
- 12538 1J **Trustworthy agents under a veil of misinformation: mechanism design under adversarial upstream conditions** [12538-46]
- 12538 1K **Exploring new strategies for comparing deep-learning models** [12538-53]
- 12538 1L **Optimizing machine learning inference performance on IoT devices: trade-offs and insights from statistical learning** [12538-54]
- 12538 1M **Unsupervised synthetic image refinement via contrastive learning and consistent semantic-structural constraints** [12538-56]
- 12538 1N **Detecting functional objects using multi-modal data** [12538-57]
- 12538 1P **End-to-end trustworthy ML for multidomain operations** [12538-59]
- 12538 1Q **On the performance of machine learning fairness in image classification** [12538-60]
- 12538 1R **Explainability and causality for robust, fair, and trustworthy artificial reasoning** [12538-61]
- 12538 1S **Evaluating multi-agent reinforcement learning on heterogeneous platforms** [12538-62]
- 12538 1T **Cross-sectional display system using AR (augmented reality), VR (virtual reality), and MR (mixed reality) for 3D x-ray CT inspection** [12538-63]
- 12538 1U **HDA: an iterative hyperplane-search method for discriminant analysis** [12538-65]
- 12538 1W **Evaluating the efficacy of different adversarial training strategies** [12538-72]

---

**DIGITAL POSTER SESSION**

---

- 12538 1X **Denial of service detection on industrial control system using BLSTM** [12538-70]
- 12538 1Y **Spam SMS detection based on long short-term memory and recurrent neural network** [12538-71]