Preface of the 2018 Symposium on Adversary Aware Learning Techniques and Trends in Cybersecurity (ALEC) (co-located with AAAI Fall Symposium Series 2018)

Prithviraj Dasgupta, Joseph B. Collins, Ranjeev Mittu[*]

Machine learning-based intelligent systems have experienced a massive growth over the past few years, and are close to becoming ubiquitous in the technology surrounding our daily lives. However, a critical challenge in machine learning-based systems is their vulnerability to security attacks from malicious adversaries. The vulnerability of these systems is further aggravated as it is non-trivial to establish the authenticity of data used to train the system, and even innocuous perturbations to the training data can be used to manipulate the systems behavior in unintended ways. Recent reports about malicious manipulation of social media feeds masquerading as authentic news items provide compelling evidence towards developing stronger and more resilient measures for combating adversarial attacks on machine learning-based systems.

The ALEC'18 symposium was organized to address the overarching need towards making automated, machine learning-based systems more robust and resilient against adversarial attacks, so that humans can use them in a safe and sustained manner. The areas of interest of the symposium included the following topics:

- Adversary-aware Machine Learning - Reinforcement Learning, Lifelong Learning, Deep Learning
- Generative Adversarial Networks
- Adversary- aware Prediction, Forecasting and Decision Making Techniques
- Game Theory and Game Playing to counter adversarial learning
- Distributed, Multi-agent Systems
- Adversarial Issues and Techniques for Cyber-Physical Systems, Adversarial Robotics
- Operations Research related to Adversarial Learning
- Applications of Adversarial Learning
- Security Threats and Vulnerabilities of Adversarial Learning
- Human factors and adversarial learning with human-in-the-loop

The symposium included two keynote talks and ten orally presented papers. The first keynote talk titled *AI Canonical Architecture and Robust AI* by David R. Martinez from MIT Lincoln Laboratories discussed the performance assessment of AI-based systems and the need for robust AI. Xiaojin (Jerry) Zhu from the University of Wisconsin-Madison presented the second keynote titled *An Optimal Control View of Adversarial Machine Learning* on a novel control theory-based framework for representing various adversarial learning problems. The research papers presented at the symposium were grouped into three theme-based sessions: (1) Adversarial Data Generation and Adversarial Training, (2) Countering Adversarial Attacks in Cybersecurity, and, (3) Novel Approaches in Adversarial Artificial Intelligence. The symposium concluded with a group discussion on the immediate technological enablers and hurdles in adversarial learning as well as determining a roadmap for addressing longer term problems and challenges in the field.

Finally, we would like to thank the following ALEC'18 program committee members and reviewers for their support with reviewing papers and with various aspects of organizing the symposium:

- Amitabh Mishra, U.S. Army CERDEC, USA
- Abebaw Tadesse, Langston University, USA
- Krishnendu Ghosh, Miami University of Ohio, USA
- Ying Zhao, Naval Postgraduate School, USA

November 7, 2018.

Prithviraj Dasgupta
Joseph B. Collins
Ranjeev Mittu

[*] P. Dasgupta is with the Computer Science Department, University of Nebraska, Omaha, NE, USA. e-mail: pdasgupta@unomaha.edu. J. Collins and R. Mittu are with the U.S. Naval Research Laboratory, Washington D.C., USA. Email: {joseph.collins, ranjeev.mittu}@nrl.navy.mil

In: Joseph Collins, Prithviraj Dasgupta, Ranjeev Mittu (eds.): Proceedings of the AAAI Fall 2018 Symposium on Adversary-Aware Learning Techniques and Trends in Cybersecurity, Arlington, VA, USA, 18-19 October, 2018, published at http://ceur-ws.org