REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
26-01-2023	Final Report	1-Jun-2017 - 31-May-2018

4. TITLE AND SUBTITLE
Final Report: Conference and Symposia Grants: Adversarial Machine Learning Workshop

5a. CONTRACT NUMBER
W911NF-17-1-0237

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
611102

6. AUTHORS

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
Pennsylvania State University
Office of Sponsored Programs
110 Technology Center Building
University Park, PA 16802 -7000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS (ES)
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSOR/MONITOR'S ACRONYM(S)
ARO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
70681-NC-CF.1

12. DISTRIBUTION AVAILIBILITY STATEMENT
Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Patrick McDaniel
UU	UU	UU	UU		19b. TELEPHONE NUMBER 814-863-3599

RPPR Final Report
as of 27-Jan-2023

Agency Code: 21XD

Proposal Number: 70681NCCF **Agreement Number: W911NF-17-1-0237**
INVESTIGATOR(S):

Name: Patrick McDaniel
Email: mcdaniel@cse.psu.edu
Phone Number: 8148633599
Principal: Y

Organization: **Pennsylvania State University**
Address: Office of Sponsored Programs, University Park, PA 168027000
Country: USA
DUNS Number: 003403953 EIN: 246000376

Report Date: 31-Aug-2018 Date Received: 26-Jan-2023
Final Report for Period Beginning 01-Jun-2017 and Ending 31-May-2018
Title: Conference and Symposia Grants: Adversarial Machine Learning Workshop
Begin Performance Period: 01-Jun-2017 **End Performance Period:** 31-May-2018
Report Term: 0-Other

Submitted By: Patrick McDaniel Email: mcdaniel@cse.psu.edu
Phone: (814) 863-3599

Distribution Statement: 1-Approved for public release; distribution is unlimited.

STEM Degrees: **STEM Participants:**

Major Goals: Lead the creation and execution of a workshop on the then-emerging area of adversarial machine learning (otherwise known as AML).

Accomplishments: Symposium was held on September 14th, 2017.

Training Opportunities: Nothing to Report

Results Dissemination: Nothing to Report

Honors and Awards: Nothing to Report

Protocol Activity Status:

Technology Transfer: Nothing to Report

RPPR Final Report
as of 27-Jan-2023

Partners

,

I certify that the information in the report is complete and accurate:
Signature: Patrick McDaniel
Signature Date: 1/26/23 8:55AM

Final Performance Report for ARO Grant W911NF-17-1-0237

PI: Patrick McDaniel (mcdaniel@cse.psu.edu)
Computer Science and Engineering
Penn State University

The ARO workshop grant "Adversarial Machine Learning Workshop" was award to Penn State to lead the creation and execution of a workshop on the then-emerging area of adversarial machine learning (otherwise known as AML). This was the first of such workshops in the area.

Venue: The Symposium was held on September 14th, 2017 -- 9:00am - 4:30pm on the campus of Stanford University in Palo Alto, California.

Attendees: The workshop had a broad collection of attendees and speakers from many different disciplines. The program had 34 academic, 3 industrial and12 government attendees.

Support: The support helped cover meeting expenses and travel support for 9 of the speakers to attend the conference. These latter expenses were in the form of travel, hotel, and other incidental expenses.

Program: The program consisted of talks outlining the area and key research results of the time, as well as provided time to have a community discussion of the future of this research area. The keynote set of speakers includes Ian Goodfellow, Dawn Song, David Evans, and Nicolas Papernot and Tien Pham among others.

The agenda included:

Workshop Agenda

9:15 Welcome and overview
9:30-10:15 Ian Goodfellow, Google
10:15-10:45 Jacob Steinhardt, Stanford
10:45-11:00 Break
11:00-11:30 Nicolas Papernot, Penn State
11:30-12:00 Aleksander Madry, MIT
12:00-12:30 Tian Pham, ARL
12:30-14:00 Lunch
14:00-15:00 Breakouts I
15:00-15:30 Breakouts II
15:30-16:00 Dawn Song, UC Berkeley
16:00-16:30 Dave Evans, Virginia
16:30-16:35 Closing