Artificial Intelligence and Cybersecurity Workshop

The Hotel at the University of Maryland

7777 Baltimore Ave. College Park, MD 20740

June 4-6, 2019

Agenda

TUESDAY, JUNE 4

07:30 – 08:00 ARRIVAL / CHECK-IN

08:00 – 08:30 **Welcome and Charge**
John Launchbury (Galois) and Patrick McDaniel (Penn State)

08:30 – 09:15 **Plenary I: AI for Security**

The Dangers of the Subconscious Mind (of Cyber Reasoning Systems)
Yan Shoshitaishvili (Arizona State University)

09:15 – 09:30 BREAK

09:30 – 12:00 **Breakouts I: AI for Security** *(with informal break as needed)*

12:00 – 13:00 LUNCH

13:00 – 13:45 **Plenary II: Security of AI**

Individual Fairness for Machine Learning
Michael Kearns (University of Pennsylvania)

13:45 – 14:00 BREAK

14:00 – 16:30 **Breakouts II: Security of AI** *(with informal break as needed)*

16:30 ADJOURN

WEDNESDAY, JUNE 5

08:00 – 08:30 ARRIVAL / CHECK-IN

08:30 – 09:15 **Plenary III: Industry Research**
Úlfar Erlingsson (Google)

09:15 – 09:30 BREAK

09:30 – 12:00 **BREAKOUTS III: Broader questions** *(with informal break as needed)*

12:00 – 13:00 LUNCH

13:00 – 13:45 **PLENARY IV: Academic Research**

Security Against Adversarial Examples
David Wagner (University California, Berkeley)

13:45 – 14:00 BREAK

14:00 – 16:30 **BREAKOUTS IV: Writing Session** *(with informal break as needed)*

16:30 ADJOURN

THURSDAY, JUNE 6

08:00 – 08:30 ARRIVAL / CHECK-IN

08:30 – 09:15 **PLENARY V: Government Mission Context**

Mona Lisa Talks
Dean Souleles (Office of the Director of National Intelligence)

09:15 – 09:30 BREAK

09:30 – 11:45 **Poster Session**

11:45 – 12:00 **Thanks and Adjourn**