The National Academies of
SCIENCES • ENGINEERING • MEDICINE

Computer Science and Telecommunications Board
Intelligence Community Studies Board

Workshop on the Implications of Artificial Intelligence and Machine Learning for Cybersecurity

March 12-13, 2019

National Academy of Sciences, Room 125
2101 Constitution Ave NW
Washington, DC 20418

Day One
Tuesday, March 12

WORKSHOP INTRODUCTION AND CONTEXT

9:00 – 9:15 AM	**Welcome** Fred Chang, Workshop Chair, Southern Methodist University
9:15 – 9:30	**Remarks from Workshop Sponsor** Vinh Nguyen, Representative of the Sponsor
9:30 – 10:15	**Current and Emerging AI Capabilities and Research** Subbarao Kambhampati, Arizona State University
10:15 – 10:30	Break

ARTIFICIAL INTELLIGENCE AND CYBERSECURITY OPERATIONS

10:30 AM – 12:00 PM	**Currently Deployed AI/ML Tools for Cyber Defense Operations** *Moderator: John Manferdelli, Northeastern University* Sven Krasser, Crowdstrike Dave Baggett, INKY Alex Kantchelian, Google
12:00 – 1:30	Working Lunch
1:30 – 3:00	**Adversarial AI for Cybersecurity: R&D and Emerging Areas** *Moderator: Wenke Lee, Georgia Institute of Technology* David Martinez, Lincoln Labs Yevgeniy Vorobeychik, Washington University Una-May O’Reilly, Massachusetts Institute of Technology

3:00 – 3:15	Break
3:15 – 4:50	**Security Risks of AI-Enabled Systems** *Moderator: Phil Venables, Goldman Sachs* Nicolas Papernot, Google Brain Bo Li, University of Illinois at Urbana-Champaign Zico Kolter, Carnegie Mellon University
4:50 – 5:15	**Discussion: The Utility and Potential of AI/ML for Cybersecurity**

Day Two
Wednesday, March 13

UNDERSTANDING OFFENSIVE OR MALICIOUS APPLICATIONS OF AI

9:00 – 9:05 AM	**Welcome** Fred Chang, Workshop Chair
9:05 – 10:45	**The Use of AI/ML in Cyberattacks** *Moderator: Kathleen Fisher, Tufts University* David Brumley, Carnegie Mellon University Tyler Moore, University of Tulsa Wyatt Hoffman, Carnegie Endowment for International Peace
10:45 – 11:00	Break
11:00 AM – 12:00 PM	**Security Implications of Deep Fakes and Synthetic Media** *Moderator: Subbarao Kambhampati, Arizona State University* Jay Stokes, Microsoft Research Delip Rao, AI Foundation
12:00 – 1:00	Working Lunch
1:00 – 2:30	**Discussion: Identifying Key Implications and Open Questions**
2:30	Adjourn