NATIONAL ACADEMIES Sciences Engineering Medicine

https://www.nationalacademies.org/

AGENDA

Transformative Science and Technology Seminar Series for the Department of Defense

AI and Large Language Models: New Advances and Attack Surfaces

December 12, 2023

NAS 125

1:00	Welcome Remarks → Alton Romig, Executive Officer, National Academy of Engineering → Bindu Nair, Director of Basic Research, U.S. Department of Defense
1:10	U.S. Long- Term Competitiveness in AI for National Security → Ylli Bajraktari, President and CEO, Special Competitive Studies Project
2:00	Adversarial Attacks on Large Language Models → Zico Kolter, Professor of Computer Science, Carnegie Mellon University; Chief Scientist of AI Research, Bosch Center for AI
3:00	Coffee Reception

NATIONAL ACADEMIES Sciences Engineering Medicine

https://www.nationalacademies.org/

SPEAKER BIOGRAPHIES

Dr. Alton D. Romig, Jr. is the executive officer of the National Academy of Engineering. Under Congressional charter, the Academy provides advice to the federal government, when requested, on matters of engineering and technology. As executive officer, Dr. Romig is the chief operating officer responsible for the program, financial and membership operations of the Academy, reporting to the NAE president. He was previously vice president and general manager of Lockheed Martin Aeronautics Company Advanced Development Programs, better known as the Skunk Works ®. He spent the majority of his career at Sandia National Laboratories, operated by the Lockheed Martin Corporation, having joined Sandia as a member of the technical staff in 1979 and moved through a succession of R&D management positions leading to appointment as executive vice president in 2005. He served as the deputy laboratories director and chief operating officer until 2010 when he transferred to the Skunk Works. Dr. Romig serves or has served on a number of Advisory Committees including those at Univ of Washington, MIT, Ohio State, Purdue, Georgia Tech, the Colorado School of Mines and Sandia National Laboratories. He is also visiting Associate of Applied Physics and Materials Science at Cal Tech. Dr. Romig is a member of the Board of Directors of Football Research, Inc., a non-profit entity created and supported by the National Football League to review engineering technology to improve the safety of the sport. From 2003 to 2008, he served on the Board of AWE, Aldermaston, UK and chaired the Program committee. Dr. Romig is a Fellow TMS, IEEE, AIAA and AAAS. He is also a Fellow and Honorary Member of ASM International. Dr. Romig was elected to the National Academy of Engineering in 2003 and the Council of Foreign Relations in 2008. He was awarded the ASM Silver Medal for Materials Research in 1988. Dr. Romig graduated from Lehigh University in 1975 with a BS in Materials Science and Engineering. He received his MS and PhD in Materials Science and Engineering from Lehigh University in 1977 and 1979, respectively.

Dr. Bindu R. Nair is the Director of Basic Research within the Office of the Secretary of Defense (OSD). She is responsible for oversight and coordination of the Department's $2.5 billion annual investment in basic science. This investment supports high risk and high pay-off basic research projects in many fields spanning the physical sciences, life sciences, environmental sciences, applied mathematics, to name a few, that probe the limits of today's technologies and aim to discover new phenomena and develop the know-how that may ultimately lead to future technologies. Bindu previously served in a number of roles at DoD, including Acting Director and Deputy Director in the Human Performance, Training and Biosystems Directorate within the Office of the Secretary of Defense. In this role, she was involved in overseeing a broad range of DoD's science and technology programs. Her specific areas of responsibilities in the office were in environmental technologies, bio-assist technologies (exoskeletons and prosthetics), human machine teaming, and social behavioral modeling in the information environment. Bindu earned a BSc at the University of Florida and a PhD in Materials Science and Engineering at MIT.

Mr. Ylli Bajraktari is the President and CEO of the Special Competitive Studies Project. Prior to launching SCSP, Ylli served as the Executive Director of the National Security Commission on Artificial Intelligence. Prior to joining NSCAI, he served as Chief of Staff to the National Security Advisor LTG H.R. McMaster held a variety of leadership roles for former Deputy Secretary of Defense Robert Work, and served as Special Assistant to the Chairman of the Joint Chiefs of Staff, General Dempsey. Originally joining the Department of Defense in 2010, he served in the Office of the Undersecretary for Policy as a country director for Afghanistan, and later India. Mr. Bajraktari is the recipient of the Department of Defense Distinguished Civilian Service Medal – the highest award given to career DoD civilian employees. Ylli received his undergraduate degree from The George Washington University and master's degree from Harvard University.

Dr. Zico Kolter is an Associate Professor in the Computer Science Department at Carnegie Mellon University, and also serves as chief scientist of AI research for the Bosch Center for Artificial Intelligence. His work spans the intersection of machine learning and optimization, with a large focus on developing more robust and rigorous methods in deep learning. In the context of robust machine learning in particular, his group developed several early methods for certified robustness, including convex relaxations for verifying deep networks, and randomized smoothing approaches. He is a recipient of the DARPA Young Faculty Award, a Sloan Fellowship, and best paper awards at NeurIPS, ICML (honorable mention), AISTATS (test of time), IJCAI, KDD, and PESGM.