THREATCASTING WEST, 2017

May 1-2, 2017

In May of 2017 the Threatcasting Lab at Arizona State University and the Army Cyber Institute conducted Threatcasting West workshop. Threatcasting is a conceptual framework that allows multidisciplinary (public, private, and academic) groups to envision and plan against threats in the future. In it we not only describe tomorrow's threats but also identify specific actions, indicators and concrete steps that can be taken today to disrupt, mitigate and recover from these future threats.

With 47 participants from diverse organizations, we created 22 unique futures while exploring complex issues including the advancement of artificial intelligence, the diminishing ability to conduct covert intelligence gathering, the growing complexity of code, and future division of work roles between humans and machines.

CONTACT US AT THREATCASTING.COM

REPRESENTATION

47 Participants

Attending participants of Threatcasting West were a mixture of government, academic, and private industry. Strategists and practitioners from the U.S. Secret Service, NETCOM (U.S. Army Network Enterprise Technology Command), ARCIC (Army Capabilities Integration Center), ASA R&T (Assistant Secretary of the Army for Research and Technology), SOCoE (U.S. Army Special Operations Center of Excellence), ARCYBER (U.S. Army Cyber Command), and the ACI (Army Cyber Institute) represented government agencies. They were joined by academics from Arizona State University, University of Arizona, and Northeastern University as well as cadets from the United States Military Academy (West Point) and the United States Air Force Academy. From an industry perspective, futurists and technologist from Intel, Lockheed Martin, AECOM, Capital One, Illumnio, APICS, ISACA, Fractal Industries, Soar Technology, Strategic Foresight Partners, and BaldFuturist provided expertise and a wide range of diverse perspectives. All attendees worked in small, collaborative, cross-industry groups to model futures taking place in the year 2027.

INPUTS

Worksession Expert Interviews

Six curated inputs from cross-industry experts helped inform the futures we modeled. First was Dr. Genevieve Bell, discussing how we should think about interrogating AI. Sam Harris posed the question of how we might build AI without losing control over it. Dr. Dave Gioe outlined 14 cyber considerations for humans. Paul Thomas discussed how to approach Threatcasting from an economic perspective. Andre LeBlanc outlined the growth, impact, and future of applying AI to real world industries. The sixth and final talk was MAJ Natalie Vanatta, PhD with a wrap up of key ideas from various expert interviews regarding cyber growth and our relationship with machines. Transcripts of all talks will be made available in the final technical report.

Dr. Genevieve Bell: https://www.youtube.com/watch?v=F_QZ2F-qrGM&t=

Sam Harris: https://www.ted.com/talks/sam_harris_can_we_build_ai_without_losing_control_over_it#t-852226

Dr. Dave Gioe: https://vimeo.com/214907268/161dd79e22

Paul Thomas: https://www.youtube.com/watch?v=PWkS3Ga4J6Q&feature=youtu.be

Andre LeBlanc: https://www.youtube.com/watch?v=xH_B5xh42xc