



ARMY CYBER INSTITUTE

AT WEST POINT

From Science Fiction to the Future of Artificial Intelligence

The New Dogs of War: The Future of Weaponized Artificial Intelligence envisions future threats and solutions

West Point, NY: A new report from the Army Cyber Institute at West Point and Arizona State University contemplates future threats the United States may face from the advent of artificial intelligence. Focused on weaponized AI—artificial intelligence used as a weapon, intentionally or otherwise—the report examines how next-generation threat actors could use AI and advanced machine learning techniques against the U.S. military, government, industry, and private citizens. The complete report and executive summary are available for download from <http://threatcasting.com/events/event/threatcasting-workshop-west-2017/>

The report identified three key threats surrounding weaponized AI: surveillance and coercion, the AI weapons factory, and the careless destabilization of national security. Whereas traditional weapons have generally been easily defined and identified and tracked through straight forward processes, weaponized AI presents new challenges, not least that many potential future usages of AI are intended for non-military purposes.

The report also discusses the actions necessary by academia, non-profits, industry, government, and individuals to mitigate, disrupt, or recover from possible threats: further research, technical and process tools, and regulation and oversight. These actions constitute a whole-of-society approach to problem solving and have been applied to specific domains including detailed steps.

The report is based on a May 2017 workshop hosted by Arizona State University, *Threatcasting West 2017*, and run by the Threatcasting Lab, a joint endeavor between ASU and the Army Cyber Institute. The event brought together individuals from across the military, government, academia and private industry to envision possible threats ten years in the future and identify actions to identify, track, disrupt, mitigate, and recover from possible threats.

Known as *Threatcasting*, this conceptual framework and process enables multidisciplinary groups to envision and plan systematically against future threats. Over the course of two days, 47 participants created 22 unique threat futures, exploring the advancement of AI, the diminishing ability to conduct covert intelligence gathering, the growing complexity of code, and future division of work roles between humans and machines.

Media representatives interested in Threatcasting should contact:

Terence M. Kelley
The Army Cyber Institute at West Point
terence.kelley@usma.edu
(845) 667-7065
@ArmyCyberInst

Denise Kronsteiner
School for the Future of Innovation in Society
Arizona State University
denise.kronsteiner@asu.edu
(480) 727-6193

Register now for *CyCon U.S., the International Conference on Cyber Conflict*, Nov. 7-8, 2017 in Washington D.C.:
http://aci.cvent.com/cycon_us.