November 21, 2019

CSET Launching Cybersecurity and AI Project
New Hewlett Foundation Grant to Support Cutting-Edge Research

Washington, DC - Accelerating threats to cybersecurity, the impact of automation on cyber defense, and the degree to which cyber operations will become faster and more powerful are among the subjects that the Center for Security and Emerging Technology (CSET) will now start to explore thanks to a grant from the William and Flora Hewlett Foundation.

The $2 million grant will support CSET's new Cybersecurity and AI project (CyberAI). The Principal Investigator for this grant and for the CyberAI project is Ben Buchanan, the center's senior faculty fellow and an Assistant Teaching Professor at Georgetown University.

CyberAI will feature a core of fellows and staff dedicated to examining the ways in which ever-increasing automation affects the world of cyber offense and defense. Its key research questions include the degree to which cyber defense might be meaningfully improved, the increased risk of accidental damage and escalation, and the implications for strategic stability between nations.

"Automation can do more than make cyber operations go faster. It can supercharge their ability to spread, amplifying their effectiveness and potency," Buchanan noted. "AI holds promise for cyber defense as well. If AI can improve detection, it can dramatically reduce the dangers that cyber operations might bring. There's a lot of hype out there, and our job is to cut through it and find the most important facts and ideas.

"Four dimensions of cyber operations—speed, offensive power, defensive potential, and accident risk—are fundamental to achieving the goals of our program. They relate directly to both the technical and geopolitical dimensions of cybersecurity. In our view, it will be difficult to make progress on core cybersecurity challenges without reckoning with the risks and rewards of automation. Furthermore, we will be interested in the cybersecurity of AI systems themselves, especially with the rise of adversarial learning."

Established in January 2019, CSET is a research organization focused on studying the security impacts of emerging technologies, supporting academic work in security and technology studies, and delivering nonpartisan analysis to the policy community.

"The CyberAI project will build on CSET's strengths: the rigor of our research, our reputation for thorough and impartial analytical products, and our growing data science capabilities," Matheny said. "We are grateful to the Hewlett Foundation for recognizing the importance of cybersecurity's intersections with AI, and for their confidence in our ability to deliver results."