October 22, 2019

Artificial Intelligence and Cyber Threats: CSET Expert Testifies to Congress on Vulnerabilities and Need for Defense Using Latest AI Tools

Washington, DC – Artificial intelligence will alter the nature of cyber attacks and defense, but will not replace the human element in cyber operations, according to Ben Buchanan, Senior Faculty Fellow at the Center for Security and Emerging Technology (CSET). Buchanan testified today before the House Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation in a hearing entitled, "Preparing for the Future: An Assessment of Emerging Cyber Threats."

In his testimony, Buchanan identified three dimensions of artificial intelligence and cybersecurity deserving further analysis:

- AI systems are susceptible to traditional software vulnerabilities but also have unique vulnerabilities to "adversarial learning."
- Automation has changed the nature of offensive cyber attacks against regular computer systems, resulting in some of the most damaging cyber attacks to date.
- Developing AI-enabled tools for cyber defense is imperative.

Buchanan concluded his remarks by emphasizing that cyber operations are fundamentally human operations. "For as much as we will talk about technology today," he said, "we must remember that the people in our organizations are key to addressing these threats."

Buchanan is an Assistant Teaching Professor at Georgetown University's School of Foreign Service. He is also a Global Fellow at the Woodrow Wilson International Center for Scholars, where he teaches introductory classes on AI and cybersecurity to Congressional staff. His research specialty is how cybersecurity and AI shape international security.

Established in January 2019 at Georgetown's Walsh School of Foreign Service, CSET studies the security impacts of emerging technologies, supports academic work in security and technology studies, and delivers nonpartisan analysis to the policy community. CSET aims to prepare a generation of policymakers, analysts and diplomats to address the challenges and opportunities of emerging technologies. During its first two years, CSET is focusing on the effects of progress in artificial intelligence and advanced computing.