

Questions for the Record from Representative Darrell Issa for Dr. Benjamin Jensen
Protecting Our Edge: Trade Secrets and the Global AI Arms Race
May 7, 2025

1. What is data poisoning, and how might it be used to counter malign foreign actors from engaging in economic espionage against U.S. AI companies? Are there any historical examples of using such techniques to discourage IP theft, and if so, were they successful in the long term?
2. The PRC leverages both willing and unwilling participants in order to steal technology from U.S. companies and labs, including through recruiting programs like the Thousand Talents Program, as well as more sinister methods, such as threatening family members. How can such aggressive actions be countered?