AMERICAN FOREIGN
POLICY COUNCIL

# Defense Technology Program Briefing: Cyber Crime

May 14, 2015

**Related Categories:** Cybersecurity and Cyberwarfare; Democracy and Governance; Science and Technology
**Related Expert:** Richard M. Harrison

On May 14, AFPC held the third installment of its Defense Technology Program's five-part "Understanding Cybersecurity" briefings for Congressional staffers.

The event focused on Cyber Crime, and discussed law enforcement and regulatory action to either pursue attackers or assist victims. The event, moderated by AFPC Director of Defense Technology Programs Rich Harrison, included presentations by Matthew Noyes, a Cyber Policy Analyst for the U.S. Secret Service; Trey Herr, a senior research associate with the Cyber Security Policy and Research Institute and a PhD candidate in political science at George Washington University; and Dr. Sasha Romanosky of the RAND Corporation.

The experts emphasized that cyber crime encompasses a wide range of activities that includes theft, fraud and harassment; stealing valuable intellectual property as part of industrial espionage; committing financial fraud and credit card theft; and disrupting Internet services for ideological goals ("hacktivism"). One approach in combatting cyber crime is to attack the reputation mechanisms, disrupting the tenuous chains of trust that link buyers and sellers for malicious software and stolen information.

Speakers cautioned that attempting to force firms to increase cyber security should be balanced with inducing consumers to take appropriate security and privacy precautions. They also explained that the comparative security posture of various firms and agencies can influence target selection by these criminals, and concluded that successful cyber attacks can therefore be considered a result of mismatched investment in information security.