AMERICAN FOREIGN
POLICY COUNCIL

Understanding Cybersecurity - Part 3 | Cyber Crime

June 29, 2015 **Richard M. Harrison**

Related Categories: Cybersecurity and Cyberwarfare

On May 14, AFPC held the third installment of the AFPC Defense Technology Program's five-part Understanding Cybersecurity lunch briefing series for Congressional Staffers. The event was focused on Cyber Crime, which discusses law enforcement and regulatory action to either pursue attackers or reform victims. The event provided a basis for understanding the cyber crime and the prosecution of cybercriminal groups, asset seizure, data breach notification, and standards for reporting cyber incident.

AFPC Director of Defense Technology Programs moderated the event. The guest speakers were cyber security experts Mr. Matthew Noyes, Mr. Trey Herr and Dr. Sasha Romanosky. Mr. Noyes serves as a Cyber Policy Analyst for the U.S. Secret Service where he focuses on criminal investigation. His background also includes experience as a cybersecurity consultant at Good Harbor Consulting and as an officer in the U.S. Army where he served in Germany and Iraq. Mr. Trey Herr is a senior research associate with Cyber Security Policy and Research Institute and a PhD candidate in political science at George Washington University. He consecutively works as an adjunct researcher at the Institute for Defense Analysis. Dr. Sasha Romanosky is an associate policy researcher at the RAND Corporation. He was a Microsoft research fellow in the Information Law Institute at New York University, and was a security professional for over 10 years within the financial and e-commerce industries at companies such as Morgan Stanley and eBay.

The experts defined cyber crime as 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"). They stated that the relative security posture across firms and the cost of acquiring and implementing malicious software (i.e., malware) can influence target selection by these criminals. And explained that successful cyber attacks can therefore be considered a result of mismatched investment in information security.

There are ways to combat cyber crime, one approach may be to attack the reputation mechanisms [user review systems within the cyber black market], disrupting the tenuous chains of trust that link buyers and sellers for malicious software and stolen information. Alternately, the data collected by insurance carriers affords them a unique advantage over any other entity— even government agencies—when it comes to assessing the benefits of different information assurance controls and practices. The speakers' cautioned that discussions regarding policies or regulations to force firms to increase cyber security should also be balanced with discussions of inducing consumers to take appropriate security and privacy precautions.

To access the full report in its entirety, please read the downloadable file below.