AMERICAN FOREIGN POLICY COUNCIL

Defense Technology Program Briefing: "Going Dark — Implications of an Encrypted World: Understanding the encryption debate, its effect on U.S. national security, and options for legislation."

February 27, 2017

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

On February 27, AFPC's Defens gressional Staff in the House and Senate on the encryption debate ding the encryption debate, its effect on U.S. national security, a

Amb. Robert Galucci, Dr. James Clad, AFPC Director for Asian Security Programs Jeff M. Smith, and Congressman Ted Poe (R-TX), d iscuss the dual challenges of Pakistani terrorism and nuclear weapons at a briefing in the U.S. House of Representatives for congressional staff.

AFPC Defense Technology Program Director Rich Harrison moderated the event with panelists including Dr. Abraham Wagner, who has spent 30 years in various posts across DoD and intelligence community and is a Lecturer in Law at Columbia Law School; Immunity Inc. CEO and former NSA Computer Security Scientist David Aitel; and QxNch Cyber Security Policy Specialist and former Director of Government Affairs at HackerOne Mara Tam.

The briefing addressed the growing use of encryption technologies to protect data. In the transition from an analog world to a digital one, users have lost control over their data as antiquated media have been replaced by digital files on systems vulnerable to "hacks" as well as surveillance programs and commercial data exploitation. At the operational level, increased used of encryption poses critical problems for legitimate intelligence and law enforcement requirements.

The discussion focused on the existing legal regime for encryption as well as the technology base supporting this aspect of cybersecurity. Possible options for intelligence and law enforcement were also discussed along with developing a useful framework to help enact appropriate legislation.