AMERICAN FOREIGN POLICY COUNCIL

Understanding Cybersecurity - Part 4 | Internet Security Governance

October 1, 2015 **Richard M. Harrison**

Related Categories: Cybersecurity and Cyberwarfare

On September 22, the AFPC Defense Technology program held a lunch briefing for Congressional staffers on Internet Security Governance as part of the five-part briefing series on the issue of cybersecurity. AFPC Director of Defense Technology programs, Rich Harrison moderated a panel of speakers including: Mr. Richard Barnes, the Security Engineering Lead at Mozilla; Mr. Trey Herr, a senior research associate at the Cyber Security Policy and Research Institute and PhD candidate in political science at George Washington University and non-resident fellow with the Cybersecurity Initiative at New America; and Ms. Heather West, who works on the public policy team for CloudFlare Inc., a content delivery network and domain name services company.

The Internet crosses national and jurisdictional boundaries, so to take legal action outside of our borders or implement new protocols can require the involvement of other state and non-state actors. The event's focus on Internet Security Governance covered technical and legal security issues that require the involvement of more than a single country. Panelists discussed defensively oriented topics including international agreements, like the Wassenaar Arrangement, and the process of drafting, approving, and promulgating security standards for implementation across the Internet.

The speakers specifically mentioned the importance of uniformity when countries craft their cyber laws. If multiple countries can adopt similar cyber governance laws, adaption by industry will be much easier. One major problem is that when the Internet was originally created security was not a concern, which has led to the vulnerabilities present today. As the Internet moved beyond select industries into the mainstream, security protocols were not well fleshed out or developed. This dynamic has led some lawmakers to think they can initiate a security Internet using a “top-down” process. However, panelists disagreed with this argument and stated that best Internet security protocols have come from industry, rather than government. Citing Google's, Mozilla's, and Microsoft's cooperation when it came to the recent change in website browser's encryption protocol. This change will cover a huge percentage of the Internet, and government involvement was not needed.

The speakers also talked about the difficulties posed by Internet giants including China and Russia. China and Russia are very interested in monitoring and controlling interactions online and allowing law enforcement agencies to have unfettered access to individual's information. Also regarding international considerations, the panelists stated that it is necessary to alter the Mutual Legal Assistant Treaty, which allows various countries access to foreign data for a domestic prosecution of an information technology crime. Currently, the length of time it takes for countries' requests to be processed is over ten months, greatly impeding investigations. Reforming the MLAT laws will lead to greater cooperation on cyber-governance issues in the future between countries.

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