AMERICAN FOREIGN POLICY COUNCIL

Understanding Cybersecurity - Part 5 | Military Cyber Operations

November 9, 2015 **Richard M. Harrison**

Related Categories: Cybersecurity and Cyberwarfare; Military Innovation

On November 10, AFPC's Defense Technology Program hosted the final segment of the five-part briefing series on cybersecurity with an event focused on Military Cyber Operations (MCO). AFPC Defense Technology Program Director Rich Harrison moderated a panel of speakers that included: Peter Singer, Co-author of Cybersecurity and Cyberwar: What Everyone Needs to Know; Trey Herr, Senior Research Associate at the Cyber Security Policy and Research Institute; and Drew Herrick, National Cybersecurity Fellow at New America.

The MCO briefing covered the acquisition and use of cyber capabilities in both the strategic and operational realms by states and non-state actors. Specifically, how adversaries involved find and exploit vulnerabilities in software and establishing long-term access to systems in use by potential targets. The panelists discussed how at the strategic level, this could involve attacks against critical infrastructure like nuclear weapons refining or heavy industrial facilities. They explained how at the operational level, military organizations may use cyber capabilities to target enemy air defense systems. The discussion focused on outlining the threats to U.S. national security, in addition to the legal constraints and considerations the U.S. military faces in response, and an emphasis was placed on developing a useful framework to help enact appropriate legislation.

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