AMERICAN FOREIGN POLICY COUNCIL

Understanding Cybersecurity - Part 1 | Redefining Cybersecurity

January 21, 2015 **Richard M. Harrison**

Related Categories: Cybersecurity and Cyberwarfare

On January 22, as part of its Defense Technology Program educational lunch briefing series, AFPC featured a presentation by Trey Herr, Dr. Allan Friedman, and Nick Rossi on the topic of cybersecurity. AFPC's Director of Operations and Defense Technology Programs Rich Harrison moderated the event held in the Capitol Visitor's Center. The briefing content was focused on redefining the term cybersecurity to provide a fundamental understanding of various cyber concepts.

Dr. Allan Friedman is a Research Scientist at the Cyber Security Policy Research Institute (CSPRI) at George Washington University's School of Engineering. He is the co-author of *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Mr. Trey Herr is a senior research associate with CSPRI 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. Friedman and Mr. Herr outlined the complexity of cybersecurity issues through assessing four different clusters. Both speakers explained that the clusters delineate between issues with an international scope as it deals with the security of the Internet's fundamental architecture, export controls and legal action, and the categorical differences among cyber actors. The first cluster, Information Assurance, addresses securing computers and networks. This covers the technology and tactics associated with protection in addition to education and techniques used to secure applications and networks in private and public sector technologies. The second cluster, Internet Security Governance (ISG) includes all forms of international cooperation and collaboration surrounding security issues. Together, the first and second clusters focus on a defensive posture as the third and fourth clusters share an offensive focus. Herr and Friedman define Cybercrime, the third cluster, as the law enforcement and regulatory action used to pursue perpetrators of cybercrime. Between cybercrime and the final cluster, Military Cyber Operations (MCO), the key difference remains that within Cybercrime, actors may harass, disrupt or even steal information but do not cause permanent damage or harm people; within MCO, the organizations, policy and law are related to deploying destructive digital or physical effects on target computer systems or defending against such.

In conclusion of the brief, Dr. Friedman and Mr. Herr characterized each distinct issue area with unique technical and policy challenges. Each of the clusters is simple, but the issues associated are difficult to solve.

The corresponding paper serves as a basic explanatory tool for these topic clusters. Future pieces in this series will go into more detail on each cluster and highlight proposed and potential legislative avenues to implement policy solutions to the pressing problems.

To access the full report based on the speakers comments, please read the downloadable file below.