AMERICAN FOREIGN
POLICY COUNCIL

Understanding Cybersecurity - Part 2 | Information Assurance

April 14, 2015 **Richard M. Harrison**

Related Categories: Cybersecurity and Cyberwarfare

On April 15, as part of its Defense Technology Program educational lunch briefing series, AFPC featured presentations by Dr. Abraham Wagner, Trey Herr, and Eric Ormes 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 information assurance, which is securing computers and networks, including protection of critical infrastructure from cyber intrusions. The event provided a basis for understanding the information assurance aspect of cybersecurity including threats to national security and the private sector from various actors. An emphasis was placed on developing a useful framework to help enact appropriate legislation.

Dr. Abraham Wagner is an Adjunct Professor of International and Public Affairs at Columbia University and Senior Fellow at the Center for Advanced Study on Terrorism. He served 30 years in defense and intelligence fields including the Defense Science Board and the scientific advisory boards of the NSA and CIA. Mr. Trey Herr is a senior research associate with CSPRI and a PhD candidate in political science at George Washington University. He also works as an adjunct researcher at the Institute for Defense Analysis. Mr. Eric Ormes is a cybersecurity consultant for the U.S. Government and private sector and former United States Air Force Communications and Information Officer. Ormes also holds several professional certifications in cybersecurity.

Dr. Abraham Wagner explained the historical context of the cybersecurity environment that we see today. He began by outlining the evolution of modern cyberspace, beginning with the Department of Defense's (DoD) experiments in switched-packed communications and subsequent creation of ARPAnet. Al Gore's bill in FY-1990 funded the transition from ARPAnet to the Internet, which opened the net to the masses. The content of modern cyberspace and the devices used to access it are vulnerable to security threats, much unlike the early years of limited accessibility. This includes both private and government sector, but he highlighted the difficult question of who is responsible for securing the Internet?

Mr. Herr and Mr. Ormes outlined the needs and processes of securing computer networks and systems from intrusive actions. Ormes first explained the tactics used to defend network and information systems, including host- and network-based mechanisms. Network or system vulnerabilities are weaknesses that must be addressed in order to create a more secure environment. Information must be shared between the government and public sector to more efficiently deal with security threats. Herr addressed the need for critical infrastructure protection (CIP), which also falls under Information Assurance. The 16 sectors associated with industrial control systems (ICS), all of which operate in the private sector with varying security standards, are also vulnerable to cyber-attacks. He explained, there is a shortage, especially in the government sector, of skilled cybersecurity workers, but the right employees must be selected to fill defined roles. Congress has a role to play in implementing security standards and implementation.

In conclusion of the brief, Dr. Wagner, Mr. Herr, and Mr. Ormes engaged in a lively debate over the future of cybersecurity. Is there in fact a future with complete security? Furthermore, what role do individual agencies play intervening in the private sector?

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