AMERICAN FOREIGN POLICY COUNCIL

# Defense Technology Program Briefing: Cyber & Electromagnetic Threats

May 9, 2018

**Related Categories:** Arms Control and Proliferation; Cybersecurity and Cyberwarfare; Democracy and Governance; Military Innovation; Missile Defense ; Science and Technology
**Related Expert:** Richard M. Harrison

On May 9, as part of the AFPC Defense Technology Program's congressional staffer education initiative, AFPC hosted an event entitled, "Protecting Critical Infrastructure from Cyber and Electromagnetic Threats." The lunch briefing, moderated by AFPC Vice President Richard Harrison, was held in the U.S. Capitol Building. Dr. George Baker, a Senior Staffer on the Congressional Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, was first to speak, followed by Robert M. Lee, the CEO and Founder of Dragos, Inc and a former cyber warfare operations officer for the U.S. Air Force.

Both speakers emphasized that our increasingly networked and digitized society has led to an overwhelming reliance on the electrical grid and telecommunications infrastructure. As a result, we have become vulnerable to a long-term collapse of infrastructure and services caused by cyber and high-intensity electromagnetic threats. Such weaknesses have been illustrated in recent years by the foreign hacking of U.S. Department of Defense (DoD) computer systems, and by Chinese penetration of private sector U.S. defense firms.

In addition to cyber threats, the U.S. is susceptible to electromagnetic pulses (EMPs) from high altitude nuclear detonations and Geomagnetic Disturbances (GMDs) from the sun. Thus, Baker and Lee argued, as adversarial nation-states and rogue actors develop new cyberwarfare capabilities, the U.S. government must prioritize the defense of cyberspace—and formulate a comprehensive strategy to protect critical national infrastructure.

By way of solutions, Baker offered a number of cost-effective options to mitigate threats from EMP attacks and those emanating from space weather. Lee described shortcomings of cyber policy in the critical infrastructure space, and argued the U.S. should do a better job of applying some of the lessons learned during the past two years from Russian cyber attacks on the Ukrainian electric grid.