Panel Recap

2018 Intelligence & National Security Summit:
Protecting U.S. Technologies

Panel

- James J. Kren, Deputy Director, Defense Security Service
- Leslie Ledda, Ph.D., Director of R&D; Intelligence, Information and Services, Raytheon Company
- Bob Litt, Of Counsel, Morrison & Foerster
- Allan Sonstebey, Deputy Executive Director, Applied Research Lab, Penn State University
- Harvey Rishikof, Visiting Professor, Temple University (moderator)

Topic Overview

The proliferation of information in the digital age creates more innovation opportunities, but it also creates more risk. New methods are needed to counter nation states that seek to steal U.S. technologies, particularly those which can be used by the Intelligence Community.

Panel Summary

Emphasizing the connection between economic security and national security, the panelists discussed new strategies and best practices to protect emerging technologies. The intelligence services of our adversaries intensively target U.S. industry and academia because they understand how the advanced technologies they develop can advance U.S. military capabilities – and because they want to steal these technologies for their own armed forces. Cyber vulnerabilities, the globalization of business, and foreign investment present significant counterintelligence challenges for American developers of advanced technologies.
Key Insights:

- Due to the interconnectedness of government, industry, and academia, security vulnerabilities now affect every sector.
- The Defense Security Service (DSS), which is charged with protecting classified information and technologies in the hands of cleared industry, would like to promote tailored industrial security measures instead of the largely compliance-based approach that is currently in place.
- Although U.S. R&D spending – currently roughly $500 billion annually – increases 8 percent annually, China is increasing its investments in technology even faster.
- About 57 percent of students in the U.S. are foreign, which may present a problem if they are developing or stealing technologies for their own countries’ intelligence services.

Recommendations:

- All members of industry should read:
  - NCSC’s Foreign Economic Espionage in Cyberspace.
- Security must become the “fourth pillar” in the acquisition process (along with cost, schedule and performance).
- Software that protects technology should be designed to defend against cyber-attacks and strike back on their own when adversaries attempt to penetrate them.
- The United States should create incentives for foreign students to stay and continue their research in the U.S. rather than return to their home countries after obtaining their degrees.
- Academics doing applied research for the government should ensure that their university leaders are educated on counterintelligence risks and best practices.

Thank You, Sponsors and Partners:

ABOUT INSA
The Intelligence and National Security Alliance’s mission is to foster dialogue between public and private elements of the national security sector. INSA approaches this mission through a variety of means, including by organizing conferences, symposia, exercises, and other discussions. INSA also convenes government and industry experts in nine policy councils that address topics ranging from security clearance reform and insider threats to acquisition management and intelligence law.

www.INSAonline.org