Session: Cyber Security
Date/Time: April 24, 2018 / 16:30-18:00

Rapporteur:
Troy Stangarone, Korean Economic Institute of America

Moderator:
David Sanger, *The New York Times*

Speakers:
Kate Brannen, *Just Security*
Neal Pollard, PricewaterhouseCoopers LLP
Michael Sulmeyer, Harvard Kennedy School Belfer Center
Richard Weitz, Hudson Institute

Session Sketch:
The Cyber Security session looked at cyber technology, a relatively new tool with the potential to disrupt the liberal international order. The panelists claimed that norms of behavior have not been established in all areas of cyber. On issues of internet freedom, such as the control domain names, there has been progress on extending the scope and influence of the liberal international order. However, norms of self-restraint have not been established when it comes to the peacetime usage of cyber tools, and they are unlikely to be established in the near future, as cyber tools have low barriers to entry, offer significant gains for states, and their use has a low risk of being punished. The panelists argued that North Korea has exploited offensive cyber operations for these reasons.

* *The views expressed herein are summaries and may not necessarily reflect the views of the speakers or their affiliated institutions.*

According to the panelists, deterrence against cyber attacks is also difficult due to the wide range of vulnerabilities, but in more conventional conflicts cyber attacks can serve as both a deterrent and a means for escalating a conflict. Cyber tools can deter conflicts when states are unsure of potential opponents’ capabilities, but using cyber tools during a conventional conflict could lead to escalation as countries seek to use weapons before command and control functions are interrupted.

The panelists further explained how the use of cyber tools has not evolved as planners initially expected. Instead of a digital “Pearl Harbor” that shut down key systems, cyber tools have been used to steal money and information, while eroding trust in systems. The session ended by highlighting the challenges in dealing with cyber going forward. Digital dangers are increasingly becoming physical dangers as more devices are connected and the costs to individuals becomes clearer, while as attacks that have become common also erode trust in cyber technology.

* *The views expressed herein are summaries and may not necessarily reflect the views of the speakers or their affiliated institutions.*