Session 6: Cyber Security Awareness and Norm-development: Practical issues for Engaging Critical Private Actors
(Friday, 11:00 AM – 12:30 PM)

Chair: Chris Demchak.
Panel members: Greg Rattray, Andrew Cushman, Rafal Rohozinski, and Bill Studeman.

Given the massive role played by private firms in most westernized democracies' national critical infrastructures, it is more effective for the nation's resilience and socio- technical- economic long-term wellbeing if these key private actors voluntarily and collectively collaborate in ensuring the whole system's cyber security.

To date, there is much talk but poll after poll suggests limited conviction across the majority of key major private firm leadership that cybersecurity is a major problem for them and their firm, let alone for the national system surrounding them. Consistently, a significant proportion of senior respondents in surveys deny knowledge that their firm has been compromised, that their bottom line is being harmed or should be modified to serve the well-being of e whole system, or that they need do more than hire outside cyber security firms to do anything more collective or unusual. (See a recent poll by Countertack).

This panel investigates how concern for the well-being of the whole national system can be made evident to, relevant for, and actionable by the major private actors. The private sector's daily practices and internal norms about cyber security are cumulatively critical for the cyber well-being of all democratic societies. A secure, national cyber future depends on the coordinated, collective willingness, knowledge, and actions of private actors in concert with public institutions.

Questions guiding panel prepared remarks:

1. (Framing) How can the C-suite and top managers of businesses in critical infrastructure and strategic economic sectors be motivated to respond to critical national security challenges?
2. (Analyzing) How can enterprise cyber security be reformulated as a value proposition for customers and a profit center for firms that enhance return on investment?
3. (Instantiating) What technology changes are necessary to enable firms to better defend their operations and intellectual property with positive side effects of enhancing national resilience?
4. (Monitoring) What innovative approaches can help forge effective public-private partnerships to overcome the cyber defense public goods dilemmas?
5. (Consequence Recognition) How can national progress be measured for reducing systemic cyber risk, enhancing cyber resilience, or mitigating strategic economic losses?
6. (Recommendations for Actions) In what programs could democracies internally and externally distribute fairly and effectively the burden of systemically ensuring cyber security for themselves and their wider community of like-minded nations?