Session 2: Norms for Military Operations in Cyberspace (Thursday, 10:45 – 12:15)
Roundtable: Chris Demchak (moderator), Jack Goldsmith (co-moderator), Suleyman Anil, Charles (Chuck) Barry, David Mussington

1. Can norms for the militaries effectively operate in a world in which attribution is hard across large volumes of attackers and cyberspace pathways, and clearly defined bad behavior thresholds are currently difficult to establish? What is the relationship between norm development and enforcement, on the one hand, and the legal removal of the anonymity of bad actors on a global scale, on the other.
2. Can international norms be achieved in a world of clashing national interests? Can, for example, the USG/DOD expect to embed norms that reflects its interests (e.g. government espionage OK, disruption of content filtering OK, commercial espionage bad, attacks on civilian infrastructure bad, etc.), or must the norms reflect the interests of other nations as well? What might this compromise position look like if (a) only state level adversaries are considered, and if (b) the wider global cyber environment of high volume uncontrolled non-state actors are taken into account?
3. How feasible today is the widely proposed norm of state responsibility for attacks emanating from a nation, regardless of attribution? How would such a scheme be implemented under current circumstances? How different would these feasibility and implementation assessments be if a process of building borders in cyberspace (cyber Westphalia) were well along?
4. What are the international norms that govern global cyber operations at the moment and how have they originated? Do other nations with a significant offensive cyber-capability take legal norms as seriously as the USG, and if not what are the consequences?
5. To what extent is the role of the military limited only to external threats with a kinetic potential clearly definable in operational redlines or conflict thresholds or does any nation's military have obligation to ensure national security by monitoring, alerting, or possibly disrupting external intrusions by bad or wicked actors into critical nonmilitary societal sectors? For example, how and to what significance do the innovations and for-hire aspects of international cybercrime contribute to a nation's decline in critical cybered systems resilience such that defense institutions need be involved proactively?
6. Need militaries be restructured for conflict in a heavily cybered world, and, if so, how? How do these recommendations change if the globe's cyberspace is relatively unfenced as it is today, or if the world has progressed far in erecting the building blocks of national borders in cyberspace?

See also Jack Goldsmith's response to the NYTimes story on the aborted cyber attacks in Libya.