Session 3: Cybercrime (Thursday, 1:00 PM – 2:30 PM)
Roundtable: Steven Chabinsky (moderator), Corey Dvorkin, Marc Goodman, Duncan Hollis, John Savage

1. What's happening now? The Council of Europe Convention on Cybercrime goes further than any other international code between nations (adopted or proposed) in harmonizing national cyber crime laws, requiring the collection and preservation of digital evidence, and fostering cooperation in criminal investigations involving computer data. Still, the cybercrime problem keeps getting worse. Some would argue that the COE Convention demonstrates that norms between nations are not a significant part of the cybercrime solution. Others would defend the Convention, stating that it simply needs to be more widely adopted and expanded in certain ways.
    - As a general proposition, how much of the cybercrime problem do you believe can be addressed through norms between nation states if the underlying attribution problem (excuse?) is not resolved first through technology and standards?
    - Would it make a difference if China and Russia, and every other country for that matter, ratified the Convention?
    - The Convention tends to be a very reactive approach to cybercrime -- the event occurs, and investigations receive international assistance. How can we make norms that are more preventive?
    - The Convention focuses on identifying and catching criminals, but does not focus on identifying cybercrime techniques with a focus on cooperation in changing architectures or standards; should that be added?
2. Are governments as important as they think they are? Or, will the private sector solve this without us?
    - Current norms focus on government to government communications and investigations. Should governments be focused instead on developing, enlisting, and enabling industry, NGOs, and citizens to help investigate cybercrime on a real-time basis and forward information appearing to pertain to the commission of a crime across borders without legal process?
    - Should governments focus on agreeing to norms amongst intermediaries, whether individual ISPs or groups like the Forum of Incident Response and Security Team/FIRST) for the rapid sharing of information, the denial of certain criminal activity occurring on their systems, the passage of investigative information across the chain of a transaction, and the establishment of duties of care and assistance?
    - What are appropriate government responses when a nation state denies assistance?
      -- Should there be a duty to assist individuals as well as nation states (e-SOS?)
      -- Is transborder search and seizure without host country approval both necessary and a non-starter?
    - What are appropriate private sector responses when their own country or another denies assistance? Will the private sector resolve this without governments? Are we going to see a rise in cyber vigilantism/hackbacks (and, if so, will host nations prosecute them? Is it time to bring back Letters of Marque?

3. How can cooperation become more agile and meaningful, whether between governments or the private sector in quickly identifying cybercrime and deterring the criminals?
    - A 24x7 network is a good start, but it's still a slow bottleneck. What other mechanisms can you envision that operate as effectively as criminals?
    - What additional confidence building measures might be effective between nation states, systems administrators, or academicians that can help better shape these efforts?
4. With regard to technologies, business practices and cultural understandings that can help reduce cybercrime.
    - Can studies of the spam value chain identify choke points that allow cooperating governments to shut down the spam activity? If so, what norms naturally follow from this observation?
    - Concerning the theft of intellectual property by individuals or organizations, can we identify the self interests of nations where these crimes occur that would encourage the nations to stop the theft? What norms would follow from this? An example might be that we should not permit our citizens to hack into international payment systems.
    - Cybercrime can involve theft of Internet traffic for commercial espionage, for example. What norms can we state on this subject?
    - Some cyber attacks, such as shutting down electric power generation on the East Coast for several days by malicious individuals, would not rise to the level of a serious nation-state cyber attack but they would be crimes. What norms can we state that would protect nations against such attacks?