- How do we design and evaluatecyberinfrastructure that takes adversary behavior, as well as normal user behavior, into account?
- This has been a goal for years. Can social scientists allow us to make progress?
  - As a process of co-design?
  - Built on theory supported by reproducible experiments?
- Understanding how the attacker adapts, and the organization adapts, is important.
  - This may not be robust across changes in society, tools, etc.
  - Probabilistic defense, layered defense, others?
- This could raise the cost of attack to no longer being worthwhile
- Criminologists, risk/game theory, anthropologists on hacker behavior, systems security, organization behavior, computational social scientist

- Structuring organizations to get the most out of cybersecurity
- Issues of governance for organizations around cybersecurity. Includes structure, process, authority, responsibility, incentives.
- There is continued differences in the roles of CIO, CSO, CISO, etc and how they function.
- We lack good data about government organizations nor how effective they have been.
  - Difference between what they say they are doing versus what they are doing.
  - Restricted publications.
- Organizational strategy, metrics and measurements, business school/MIS.
- Adam Cramer (Facebook), people at Stanford Business School

- What about cybersecurity can we inject seamlessly into our ICT infrastructure?
- We are doing a terrible job at this now.
  - Moving towards this goal is an obvious social good − this is another way to talk about usable cybersec.
  - This isn't "automatic", but rather a reduction of hassle − identifying this line is important.
- Some is changing or norms, technical work in authentication
  - role engineering, role mining that is understandable
  - Access control meeting organizational needs
- This might be more plausible if we identify some important problem or domain
- Complexities:
  - Cyber creates complexity. Security is a seam.
  - Organizations are dynamic
- Human centered security, HCI, usability studies, friendly CISOs and lawyers for ground facts, systems security, crypto

- How can one preserve individual agency in cyberspace?
- We need mental models to understand how people in different roles think about cybersecurity.
  - Roles includes CSOs, others in C-suite, adversaries, users
  - This can then be used to design systems that display behaviors that meet mental models, eg Gregg Vanderheiden's email metaphor.
- Why hard:
  - Cybersecurity is complex and abstract.
  - Privacy can contradict cybersecurity.
  - Systems will need to support personalization, high level of interaction.
- Anthropologists, HCI, accessibility.
- Gregg Vanderheiden