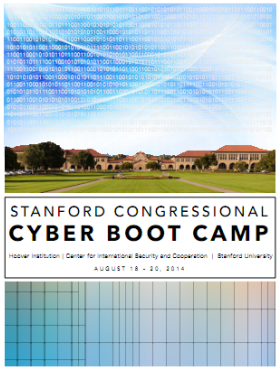
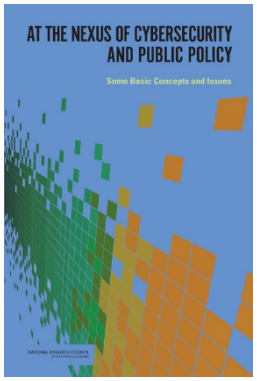
Cybersecurity Education for Policy Makers

Challenge:

- Many policy makers lack the expertise needed to make informed decisions about cybersecurity policy.
- Relevant knowledge includes economics, law, political science, psychology, organizational behavior, engineering, sociology, decision sciences, and international relations in addition to technical knowledge.
- Policy makers are a very different audience of "students":
  - little time to make considered decisions
  - Accustomed to "just-in-time" learning
  - Less willingness to engag e in intellectual struggles
  - Clear exposition preferred over Inquiry-based learning





Print examples of graphical representation of the approach to educating policy makers about key concepts and issues.

Solution:

- Production of materials tailored explicitly to policy maker questions (FAQ answers)
- Video and text based.
- "Bite-sized" chunks, to accommodate limited time and attention span

Scientific Impact:

- Contribute to solving security problems?
  - Better public policy environment for taking action to improve cybersecurity
- Improve research community's understanding of security
  - Illustrate how researchers can present their work to policy makers

Broader Impact:

- Materials are likely applicable to and usable by others with similar roles and responsibilities
  - For example, senior executives in large companies have limited attention span and time constraints.
- Materials to be made available online in due course

SaTC Award 1500089

Stanford University

John Mitchell, jcm@Stanford.edu (PI)

Herb Lin, herblin@Stanford.edu (Project Director)