Organization and Cyberinfrastructure Group

How do we design, build, evaluate, and maintain secure cyberinfrastructure that incorporate social, technical, and human aspects?

[Definition]

A secure cyber infrastructure is an integrated set of technology, systems, tools, governance, policies, and processes related to cybersecurity that aligns with the mission of the {individual, organization, or nation}.

Sub-Challenges

- How do we map cybersecurity risk for {individual, organization, or nation}?
- How do we design {framework, systems, tools, and governance} that incorporate understanding of human, organization, and adversary aspects?
- How do we collect and use cybersecurity data?
- How do we evaluate the effectiveness of the secure cyber infrastructure?
- How do we manage the cyberinfrastructure that can evolve with the dynamic interactions among human, organization, and technology?

Measurable Outcomes

- Significantly reduced data at breach incidents and costs at {individual, organizational, national} level?
- Increased compliance with cybersecurity regulations and policies at {individual, organizational, national} level?

Other ideas

- Why IT security investment has not worked effectively so far?
- How do we mitigate the risk of cybercrime?
- How do we build systems that helps learn individual users to improve 1) policy, and 2) detect attacks?
- How do system developers incorporate effective social and behavioral technics to counter denial and deception? (e.g., social engineering)