Starting points: is there a scientific way to measure security?

- If yes:
  - What would be the scientific foundation for allowing it?
    - Cyber Thermodynamics? Cyber Statistical Mechanics?
  - What experimental supports we would demand?
    - Like physics or chemistry experiments?
  - What specific measures would be?
    - E.g., Time/effort/determinedness for successful attack?
  - What kinds of research (projects) would catalyst it?

Starting points: Is there a scientific way to measure security?

- If no:
  - Why --- what is the fundamental reasoning?
    - Cyber Security Uncertainty? Cyber Security Incompleteness?
  - But can we at least reasonably approximate it (e.g., like car insurance industry)?
- Response:
  - It seems we all agree that it is doable
  - Here is how should/do we measure security

How should/do we measure security?

- Response: current practice
  - For computation-oriented security, computational complexity is a measure
  - In practice, penetration-resistance / blue-team vs. read team (ad hoc & not reproducible) / using expert systems to help measure coupled with statistical analysis within controlled environments for measuring security.
  - Economic modeling and measuring of (in)security
- Response: some possible ways to go (further)
  - What is the operational definition of security?
  - We must start with what properties we are measuring (sometimes easy to define sometimes may not be so easy to define).
  - Accountability reflects one perspective of security (by reduction)
  - Potential loss of not adopting a security mechanism (e.g., anti-virus)
  - Explicitly stating attack classes that can be defeated by a solution
  - Most current research is reactive, we need to be proactive
  - Start with specific contexts with specific measures
- Response: thinking out-of-the-box
  - Build systems with embedded security measurability
- Response: caveat
  - Numbers could be misleading
  - Need to measure/model social behavior / threat --- huge challenge