

Lesson 17:
Critical Infrastructure Protection (CIP) III:
Integration

Readings:

1. Chris Hornbarger, [*White Paper: Strategic Approach to Critical Infrastructure Protection*](#), Unpublished.
2. National Commission on Terrorist Attacks upon the United States: 344-360.
3. Chris Hornbarger, *National Strategy: Building Capability for the Long-Haul* in Russ Howard, Joanne Moore, and James Forest, eds., *Homeland Security and Terrorism: Readings and Interpretations* (New York: McGraw-Hill, 2005): the recommendation on p. 298.

Study Questions:

1. What does "integrating threat and vulnerability" mean? Why is it important?
2. What is "risk shifting," what challenge does it pose to infrastructure protection, and how should we best account for it?
3. What does "institutionalizing imagination" mean? How does it differ from "connecting the dots"?
4. Imagine that the US Government had created, prior to 9-11, a scenario that terrorists might fly airliners into large or important buildings -- not because we deemed it likely, or because we had specific intelligence indicating such an attack might be in the works, but simply because an assessment of our aviation infrastructure revealed that such an attack would probably succeed. Could such a scenario have been useful in generating "indicators" for discerning or establishing connections among available information and intelligence? How?