observations on operations/security from a (former) tier 1 builder/operator

- tool (the network) vs. experiments (the customers using the "service")
  - prior requirements work is inspiring – but need "hard" strawman use cases to guide "tool" design/build phase (think multicast effect re: IP); this effort - security examples
  - given current cost constrains – use old tech in the tool where possible / new tech where required (e.g. virtualization/partitioning)
  - as a service, think super VPN – may eases some of the security / virtualization issues
- excluding forensics, operations and security are typically a mated pair (design if not org)
  - distributed ops (organizationally) of a single network problematic; global Internet special case
  - out-of-band (OOB) constructed from the controlled network is problematic
  - as element provisioning/surveillance hard/closed and not homogeneous – partitioning and virtualization extra difficult
  - actual and virtual – ticket systems / fix agents / "remote hands"
- given state of element programmability – recognize performance realities
  - functional/logical (adequate) speed experiments --- focus here 1st (APIs)
  - higher speed experiments once (if) at-speed programmable elements can be built/acquired
- all above apply to reduced security experiment space
- old axiom: "better/faster/cheaper – pick 2"
  - GENI version? "experiment flexibility"/ "i/f simplicity" / "security/stability" / other?