[Title Here]

Your Name

[565] Words

1. Heading 1

Here is some guidance for Spring 2018 [please delete this text]:

It is important to avoid recounting the reading. Assume that everyone has read carefully, and only discuss facts/developments where relevant to your broader points. However, do feel free to define key terminology or concepts. Your response piece should follow at least one of the following strategies:

• You could analyze a major theme or problem in the readings and tie it to challenges in cybersecurity generally, or to larger theoretical frameworks used in cybersecurity.

• You could show the linkages among multiple themes/readings in the course.

• You could analyze the arguments raised in the reading by assessing strengths, the merits of counterarguments, and of course by identifying the implicit/explicit assumptions that underlie the argument. One useful exercise is to ask what would change if a key assumption changed. For instance, secrecy is a key element of cyber conflict capabilities. What might happen if we had an adversary or a condition where secrecy lost its value?

The best response pieces integrate themes of the course, pose high-level discussion questions to the group, and/or present original arguments and the limitations of those arguments.

* 1. Heading 2: Commentary Specific to Perkovich & Levite

Here are some high-level discussion questions that are raised by each chapter—feel free to use them in your response pieces or in the live discussion or to discard them:

* Are you happy with the presentation of the history/analogy?
  + Sub question: since we are not necessarily historians, what tools might you use to “kick the tires” on the analogy used?
* Is the analogy “on all fours”? Is it a good fit? Would you characterize the chapter as exploratory—as looking at the merits and demerits of the analogy, or on the other hand, does it appear to be forced?
* Is the analogy ultimately helpful? Can it be used to propose policies that cogently proceed from the analogy, or does the author invent policy prescriptions exogenous to the analogy’s contours?
* Analogies present the old “atoms and bits” problem. At core, does the analogy work, or are bits just too different from atoms for the analogy to work?
* Given what we have learned from Lapsley, should there have been a chapter in P&L about phone network hacking? What are the contours of that analogy?
  1. Commentary specific to Phil Lapsley

Here are some high-level discussion questions that are raised by Lapsley—feel free to write about them in your response pieces or raise them as discussion questions:

* What do you think of Lapsley’s method? Is it critical enough? Discuss using examples from the text.
* Did Lapsley’s history of these early hackers change your perception of current cyber problems?
* Much of the internet travels along phone network infrastructure. This means that the internet inherits some of the strengths and weaknesses of the phone network. How have the afforances of the phone network shaped modern cybersecurity problems?
* What was the fundamental security model of the phone network?
* What were the incentives of the phone system and how did these incentives shape the security of the system?
* How did competition (e.g. the entrance of MCI) affect security?
* What political and social restraints shaped the security of the phone network?
* How did competition policy (e.g. the Bell breakup) affect security?
* What insights do we gain about innovation from Lapsley?
* Does the historical account of the phone network reveal lessons for debates concerning network neutrality and privacy?
* The phone companies involved use various strategies to deter network misuse. What strategies predominate and why? Which seem most sensible? What strategies do they choose not to use, and why?
* Envelopes were not widely used until the 19th century! What might the electronic version of an envelope look like, and why don’t we see it in the telephonic network?
* Telephonic conversations have more statutory privacy protection than electronic ones (even those that traverse phone lines!). Does protection for privacy explain the deterrent strategy of telephone companies? Does privacy create unnecessary or helpful constraints on network surveillance?
* Ma Bell had a different relationship with customers (and malicious users) than your ISP or the many intermediaries that handle IP communication. What are the advantages/disadvantages of the power balance?
  1. Finally

It does help to have a section that lists specific discussion questions you woud like to raise during the session.

* + 1. Heading 3

You are a Berkeley student. Might you want to use UC Berkeley’s fonts? They are elegant. You can download them here:.

https://berkeley.box.com/s/cbhbi2gxjbkss5f4giwhn5aj6etgjths