1 Introduction

Cybersecurity and International Relations is a course designed to encourage computer scientists to think about policy and international relations issues, and to encourage political scientists to consider issues rooted in technology. Throughout the semester, students are required to submit 5 short papers in response to the week’s readings.

Students are required to turn in papers according to the due dates listed on the course website, with the responses referring to the readings available between response dates. Late papers will be not be accepted, barring emergencies.

2 Readings

- Thirteen principles to ensure enterprise system security
- The "Oceans 11" of Cyber Strikes
- Cyberwarfare: Digital weapons causing physical damage
- Exclusive: Cyberattack leaves natural gas pipelines vulnerable to sabotage
- APT and the Attack Lifecycle
- Secrets of the Comfoo Masters
- Chinese Computer Games
- A Survey of Challenges in Attribution
- Untangling Attribution
- Convention on Cybercrime

3 Criteria for Grading

- 3-4 pages, double-spaced
- 1 inch margins, 12 pt. standard font (Times New Roman, Cambria, Arial)
- Responds to one required reading (not optional or lab readings)
- Strong argument throughout, with an original thesis (not restating an author’s position) that incorporates the student’s knowledge of the subject
- Correct citations when referring to the text - in line citations or footnotes are fine - just be consistent. Use of outside sources is discouraged. If they are used, please include a bibliography so that TAs can assess their legitimacy.
- Academic language - avoid colloquial or informal language
• You are welcome to LaTex your papers!