**Thesis statement:** we aim to analyze cybersecurity. Specifically, how and where spying happens (software / hardware), how it is utilized, and what measures can be taken to prevent it.

1. Introduction to Spyware
2. History of Cisco getting busted by agencies
3. Current row with Huawei 5G infrastructure being implemented in the West
4. Segway into what is in hardware that makes it spy-friendly

II. Hardware - Routers

1. What specifically is in routers that helps them spy
2. What is a backdoor
3. Where is the data sent
4. Physical implementations of spyware
   1. Listening devices
   2. Routers with backdoors

III. Software

1. Encryption - if we encrypt our info (e-mails) does it matter if our info gets sent off to govt agencies
2. Packets - can we not see where our data packets are being sent (from observing wireshark) and if not is that why outside infrastructure is used
3. Is software embedded on our routers to send it elsewhere with us not knowing
4. Virtual implementations of spyware
   1. What vulnerabilities are manipulated
   2. How they stay hidden
   3. How they transfer information

IV. Utilization

1. How opponents use it
2. How we use it

V. Preventative Measures

1. Is there anything we can do to help ourselves
2. Encryption(what is it and how is it used)
3. Firewalls
   1. What are they
   2. Do they ever help us
   3. How can they be bypassed
   4. How to protect against spyware

VI. Conclusion

1. What can we expect in the future
2. Will spyware become harder to detect or will encryption become more efficient

VII. Resources

1. Security Engineering Third Edition: A Guide to Building Dependable Distributed Systems by Ross Anderson
2. Professor Varghese
3. UWRF Resource Database
4. TBD Resources found while gathering data and information