Plan for Research Paper’

Subjective Point:

* The main threat to our satellite infrastructure is legacy systems that would become difficult to replace and remove.

TDRS

* Relay satellites launched in the early 80s, some are still active in space and since the 1st gen was launched 2 new generations have been added since 2017.
* Old satellite need to see what security looks like for something like this.
* <https://www.nasa.gov/directorates/heo/scan/services/networks/tdrs_main>

Satellite Ground Communication

* Most frequent use of satellites, some satellites communicate to eachother in a “cross link” but a majority of them are connected and controlled via ground system.
* <https://link.springer.com/article/10.1007/s10207-020-00503-w>
* Link may have more to do with whole paper
* <https://apps.dtic.mil/sti/citations/AD1012754>
* This link is for satellite ground communication risk management

Tesla Telemetry was hacked

* Someone got access to camera’s inside of Tesla’s satellite
* SpaceX’s Starlink has resisted all attacks
* <https://www.republicworld.com/world-news/russia-ukraine-crisis/amid-russia-ukraine-war-elon-musk-says-hackers-tried-to-hack-starlink-internet-system-articleshow.html>

Unencrypted Missions

* Some missions have been unencrypted especially early on but Nasa has attempted to standardize the security.
* Tesla’s internet satellite supposedly used an unencrypted Telemetry line.

Satellite to Satellite attacks

* <https://arc.aiaa.org/doi/abs/10.2514/6.2020-4014>
* Downloaded
* Look for the book Computer and Information Security Handbook