Space and Cyber: Deterrence? In Asia?

Kazuto Suzuki

Hokkaido University

kazutos@juris.hokudai.ac.jp

Cyber as counterspace tool

- Cyber will be the central tool for counterspace
  - Increasing importance of space
  - Huge incentives for counterspace
  - Cyber would be least costly, not highly effective but could produce the result
- Protection from cyber attack
  - Cyber protection
  - Encryption
  - Teaching and training

Vulnerability in space

- Frequency
  - Scarcity of frequency – new players found it hard to find frequency allocation
  - Some university satellites uses open frequencies – easier to detect and override
  - Open the gateway for cyber attack
  - Start ups want to develop hardware with lowest cost
    - Building car without brakes
- Ground station
  - STAXNET situation – stand-off network can be contaminated by ignorance or mistake

Would it be possible to retaliate?

- Double attribution problem
  - Hard to find who is responsible for cyber attack
  - Hard to find whether cyber attack was the cause of the loss of satellite
- Tallinn manual situation
  - In war time, it is possible to retaliate as long as attribution can be established
  - In peace time, it would be difficult to retaliate even if attribution is established

Situation in Asia

- China
  - Most sophisticated cyber tech
  - Political motivations
    - Trade war
    - Taiwan issue
  - Increasing use of space – parity in space and cyber
- North Korea
  - Unpredictable strategic behavior
  - Breaking North-South, US-North dialogue
  - Least vulnerable – isolated cyber system and light use of space – retaliation may be in physical use of force